

Docket No.: 65933-082

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : Customer Number: 20277

Yoshihiro HORI, et al. : Confirmation Number:

Serial No.: : Group Art Unit:

Filed: March 26, 2004 : Examiner:

For: METHOD AND APPARATUS FOR ENCRYPTING DATA TO BE SECURED AND
INPUTTING/OUTPUTTING THE SAME

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

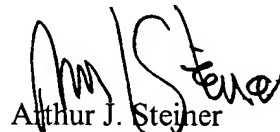
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2003-089388, filed March 27, 2003

A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY



Arthur J. Steiner
Registration No. 26,106

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 AJS:prg
Facsimile: (202) 756-8087
Date: March 26, 2004

WDC99 898520-1.065933.0082

日 本 国 特 許 庁
JAPAN PATENT OFFICE

65933-082
Hori et al.
March 26, 2004
McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 3 年 3 月 2 7 日

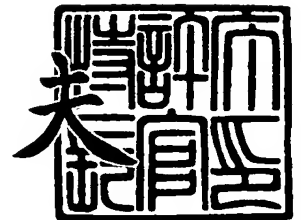
出 願 番 号
Application Number: 特 願 2 0 0 3 - 0 8 9 3 8 8
[ST. 10/C]: [J P 2 0 0 3 - 0 8 9 3 8 8]

出 願 人
Applicant(s): 三洋電機株式会社
シャープ株式会社
日本ビクター株式会社
パイオニア株式会社
株式会社日立製作所
フェニックステクノロジーズ株式会社
富士通株式会社

2 0 0 4 年 1 月 2 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



【書類名】 特許願

【整理番号】 NQC1020097

【提出日】 平成15年 3月27日

【あて先】 特許庁長官殿

【国際特許分類】 G11B 19/00

【発明者】

 【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

 【氏名】 堀 吉宏

【発明者】

 【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

 【氏名】 金井 雄一

【発明者】

 【住所又は居所】 大阪府大阪市阿倍野区长池町 2 2 番 2 2 号 シャープ株式会社内

 【氏名】 大野 良治

【発明者】

 【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 日本ビクター株式会社内

 【氏名】 大石 剛士

【発明者】

 【住所又は居所】 埼玉県所沢市花園 4 丁目 2 6 1 0 番地 パイオニア株式会社 所沢工場内

 【氏名】 多田 謙一郎

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 平井 達哉

【発明者】

【住所又は居所】 東京都千代田区丸の内 1 丁目 3 番地 1 号 東京銀行協会
ビル 1 4 F フェニックステクノロジーズ株式会社内

【氏名】 津留 雅文

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

【氏名】 長谷部 高行

【特許出願人】

【識別番号】 000001889

【氏名又は名称】 三洋電機株式会社

【特許出願人】

【識別番号】 000005049

【氏名又は名称】 シャープ株式会社

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【特許出願人】

【識別番号】 000005016

【氏名又は名称】 パイオニア株式会社

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 300017636

【氏名又は名称】 フェニックステクノロジーズ株式会社

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100105924

【弁理士】

【氏名又は名称】 森下 賢樹

【電話番号】 03-3461-3687

【手数料の表示】

【予納台帳番号】 091329

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ入出力方法、およびその方法を利用可能な記憶装置およびホスト装置

【特許請求の範囲】

【請求項 1】 データを保持する記憶装置との間でデータを入出力するホスト装置であって、

秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を複数の手順に分割し、該手順のうち前記記憶装置側で実行すべき手順を前記記憶装置に実行させるための命令を前記記憶装置に対して発行するコントローラを備え、

前記コントローラは、前記命令を発行する前に前記記憶装置から前記命令の実行に要する時間を推定するための情報を取得し、前記命令を前記記憶装置に対して発行した後、前記記憶装置が前記命令の実行に必要と推定される時間待機してから、その次の手順の命令を前記記憶装置に発行することを特徴とするホスト装置。

【請求項 2】 前記推定するための情報は、前記命令を実行するのに要する典型的な処理時間、平均処理時間、または最大処理時間を含むことを特徴とする請求項 1 に記載のホスト装置。

【請求項 3】 前記推定するための情報は、前記命令を実行するために用いられる、暗号化演算、復号演算、ハッシュ演算、乱数発生演算、およびログ検索のうち少なくとも 1 つの基本処理に要する典型的な処理時間、平均処理時間、または最大処理時間を含むことを特徴とする請求項 1 に記載のホスト装置。

【請求項 4】 データを保持する記憶媒体と、
前記記憶媒体とホスト装置との間で秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を行う際に、その暗号入出力処理を複数の手順に分割して発行された命令を前記ホスト装置から受信するコントローラと、
前記命令を実行する暗号処理部と、を備え、
前記コントローラは、前記ホスト装置からの要求に応じて、前記暗号処理部が前記命令の実行に要する時間を前記ホスト装置が推定するための情報を提供することを特徴とする記憶装置。

【請求項 5】 前記暗号入出力処理は、該処理の手順に沿って、
前記ホスト装置からデータの入力を受け、必要に応じて前記暗号処理部にて暗号化または復号を行う処理、
前記ホスト装置へデータを出力するために、前記暗号処理部にて暗号化、復号、または署名を行う処理、
前記ホスト装置へデータを出力する処理、
のいずれかの処理単位に分割され、
前記命令は、分割された処理単位ごとに発行されることを特徴とする請求項 4 に記載の記憶装置。

【請求項 6】 前記推定するための情報は、前記命令を実行するのに要する典型的な処理時間、平均処理時間、または最大処理時間を含むことを特徴とする請求項 4 または 5 に記載の記憶装置。

【請求項 7】 前記推定するための情報は、前記命令を実行するために用いられる、暗号化演算、復号演算、ハッシュ演算、乱数発生演算、およびログ検索のうち少なくとも 1 つの基本処理に要する典型的な処理時間、平均処理時間、または最大処理時間を含むことを特徴とする請求項 4 または 5 に記載の記憶装置。

【請求項 8】 データを保持する記憶装置とホスト装置との間で、秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を実行するためのデータ入出力方法であって、

前記暗号入出力処理を複数の手順に分割し、該手順のうち前記ホスト装置側で実行すべき手順を前記ホスト装置が実行するステップと、

前記記憶装置側で実行すべき手順を前記記憶装置に実行させるために、前記ホスト装置が前記記憶装置に対して命令を発行するステップと、

前記記憶装置が前記命令を受信するステップと、

前記記憶装置が前記命令を実行するステップと、を含み、

前記ホスト装置は、前記命令を発行する前に、前記記憶装置から該記憶装置が前記命令の実行に要する時間を推定するための情報を取得し、前記命令を前記記憶装置に対して発行した後、前記命令の実行に必要と推定される時間待機してから、その次の手順の命令を発行することを特徴とするデータ入出力方法。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、データ入出力技術に関し、とくに、記憶装置とホスト装置との間で秘匿すべきデータを暗号化して入出力する技術に関する。

【0002】**【従来の技術】**

近年、記憶素子の小型化、集積化、量産化が飛躍的に進み、記録媒体の小型化、大容量化、低価格化が進んでいる。そのような状況下、本出願人らは、さらに利便性の高い記録媒体の実現を目指し、従来一つのホスト装置に固定的に接続されて使用されるのが一般的であった大容量ハードディスクを、ホスト装置に着脱自在に構成することにより、複数のホスト装置でデータを共有可能なリムーバブルメディアとして扱えるようにしようと考えた。小型かつ大容量で、アクセス速度も比較的高速なハードディスクをリムーバブルメディアとして利用できることのメリットは大きい。

【0003】**【特許文献1】**

特開 2000-173158 号公報（全文）

【0004】**【発明が解決しようとする課題】**

ユーザの利便性を考えると、あらゆるホスト装置でこのリムーバブルなハードディスクを読み書きできるようにすることが望ましいが、反面、あらゆるホスト装置で読み書き可能ということは、第三者にデータが漏洩する危険性もはらんでいることを意味する。音楽や映像などのデジタルコンテンツの流通が注目される現在、著作権を適切に保護し、デジタルコンテンツの流出を防ぐためにも、秘匿すべきデータを適切に保護することのできる技術を開発することが重要である。

【0005】

本発明はこうした状況に鑑みてなされたものであり、その目的は、記憶装置とホスト装置との間で秘匿すべきデータを暗号化して入出力するときの処理効率を

向上させる技術の提供にある。

【0006】

【課題を解決するための手段】

本発明のある態様は、ホスト装置に関する。このホスト装置は、データを保持する記憶装置との間でデータを入出力するホスト装置であって、秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を複数の手順に分割し、該手順のうち記憶装置側で実行すべき手順を記憶装置に実行させるための命令を記憶装置に対して発行するコントローラを備え、コントローラは、命令を発行する前に記憶装置から命令の実行に要する時間を推定するための情報を取得し、命令を記憶装置に対して発行した後、記憶装置が命令の実行に必要と推定される時間待機してから、その次の手順の命令を記憶装置に発行する。

【0007】

暗号入出力処理を複数の手順に分割し、命令を細分化することで、バスを効率良く解放し、暗号化、復号、ハッシュ演算、乱数発生、ログ検索などの比較的時間を要する処理を行っている間に、他の命令を発行することが可能となる。暗号入出力処理に属する命令を発行した後、後続の命令を発行するまでに、前回の命令の実行が終了しているか否かを何度も記憶装置に問い合わせるのは効率が悪いので、命令の実行に要すると推定される時間だけ待機した後に、後続の命令を発行する。

【0008】

推定するための情報は、命令を実行するのに要する典型的な処理時間、平均処理時間、または最大処理時間を含んでもよい。推定するための情報は、命令を実行するために用いられる、暗号化演算、復号演算、ハッシュ演算、乱数発生演算、およびログ検索のうち少なくとも1つの基本処理に要する典型的な処理時間、平均処理時間、または最大処理時間を含んでもよい。これらの基本処理に要する時間に基づいて、命令を実行するのに要する時間を推定してもよい。

【0009】

本発明の別の態様は、記憶装置に関する。この記憶装置は、データを保持する記憶媒体と、記憶媒体とホスト装置との間で秘匿すべきデータを暗号化して入出

力するための一連の暗号入出力処理を行う際に、その暗号入出力処理を複数の手順に分割して発行された命令をホスト装置から受信するコントローラと、命令を実行する暗号処理部と、を備え、コントローラは、ホスト装置からの要求に応じて、暗号処理部が命令の実行に要する時間をホスト装置が推定するための情報を提供する。

【0 0 1 0】

暗号入出力処理は、該処理の手順に沿って、ホスト装置からデータの入力を受け、必要に応じて暗号処理部にて暗号化または復号を行う処理、ホスト装置へデータを出力するために、暗号処理部にて暗号化、復号、または署名を行う処理、ホスト装置へデータを出力する処理、のいずれかの処理単位に分割され、命令は、分割された処理単位ごとに発行されてもよい。

【0 0 1 1】

推定するための情報は、命令を実行するのに要する典型的な処理時間、平均処理時間、または最大処理時間を含んでもよい。推定するための情報は、命令を実行するために用いられる、暗号化演算、復号演算、ハッシュ演算、乱数発生演算、およびログ検索のうち少なくとも1つの基本処理に要する典型的な処理時間、平均処理時間、または最大処理時間を含んでもよい。

【0 0 1 2】

本発明のさらに別の態様は、データ入出力方法に関する。この方法は、データを保持する記憶装置とホスト装置との間で、秘匿すべきデータを暗号化して入出力するための一連の暗号入出力処理を実行するためのデータ入出力方法であって、暗号入出力処理を複数の手順に分割し、該手順のうちホスト装置側で実行すべき手順をホスト装置が実行するステップと、記憶装置側で実行すべき手順を記憶装置に実行させるために、ホスト装置が記憶装置に対して命令を発行するステップと、記憶装置が命令を受信するステップと、記憶装置が命令を実行するステップと、を含み、ホスト装置は、命令を発行する前に、記憶装置から該記憶装置が命令の実行に要する時間を推定するための情報を取得し、命令を記憶装置に対して発行した後、命令の実行に必要と推定される時間待機してから、その次の手順の命令を発行する。

【0013】

なお、以上の構成要素の任意の組合せ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【0014】**【発明の実施の形態】****(第1の実施の形態)**

図1は、第1の実施の形態に係るデータ管理システム10の全体構成を示す。データ管理システム10は、ストレージデバイス200へのデータの記録を制御する記録装置100、ストレージデバイス200に記録されたデータの再生を制御する再生装置300、およびデータを記憶保持するストレージデバイス200を備える。本実施の形態のストレージデバイス200は、データを保持する記憶媒体だけでなく、記録装置100または再生装置300などのホスト装置と記憶媒体との間でのデータの入出力を制御するコントローラなどの構成を備えるドライブ一体型の記憶装置である。本実施の形態では、ストレージデバイス200として、ハードディスクドライブを例にとって説明する。

【0015】

従来のハードディスクは、一つのホスト装置に固定的に接続されて使用されるのが一般的であったが、本実施の形態のストレージデバイス200は、記録装置100および再生装置300などのホスト装置に対して着脱自在に構成されている。すなわち、本実施の形態のストレージデバイス200は、CDやDVDなどと同様にホスト装置から取り外して持ち運ぶことができ、記録装置100、再生装置300、記録および再生が可能な記録再生装置など、複数のホスト装置間で共用することが可能な記憶装置である。

【0016】

このように、本実施の形態のストレージデバイス200は、複数のホスト装置に接続されることを前提にしており、たとえば所有者以外の第三者のホスト装置に接続されて、内部に記録されたデータを読み出される可能性もある。このストレージデバイス200に、音楽や映像などの著作権により保護されるべきコンテ

ンツ、企業や個人の機密情報などの秘匿すべきデータを記録することを想定したとき、それらの秘匿データが外部に漏洩することを防ぐためには、ストレージデバイス 2 0 0 自身にデータを適切に保護するための構成を設け、十分な耐タンパ機能を持たせることが好ましい。このような観点から、本実施の形態のストレージデバイス 2 0 0 は、ホスト装置との間で秘匿データを入出力するときに、その秘匿データを暗号化してやり取りするための構成を備える。また、秘匿データを格納するために、通常の記録領域とは異なる機密データ記憶領域を設け、その機密データ記憶領域はストレージデバイス 2 0 0 内に設けられた暗号エンジンを介さないとアクセスできないように構成する。暗号エンジンは正当な権限を有すると認証されたホスト装置にのみ秘匿データを出力する。以下、このようなデータ保護機能を「セキュア機能」ともいう。上記の構成および機能により、ストレージデバイス 2 0 0 に記録された秘匿データを適切に保護することができる。

【 0 0 1 7 】

ストレージデバイス 2 0 0 のリムーバブルメディアとしての特徴を最大限に生かすため、通常データについては、セキュア機能に非対応のホスト装置でも入出力可能とするのが好ましい。そのため、本実施の形態のストレージデバイス 2 0 0 は、従来のハードディスクとの互換性を保つべく、ANSI (American National Standards Institute) の標準規格である ATA (AT Attachment) に対応しており、上述のセキュア機能は、ATA の拡張コマンドとして実現される。ATA はシングルタスクインタフェースを採用しており、一つの命令が発行されると、その命令が終了するまでバスが占有され、次の命令を発行できない。ところが、上述のように、ストレージデバイス 2 0 0 側にも暗号通信のための構成を設け、秘匿データを暗号化して入出力するようにすると、暗号化および復号などの処理には比較的長い時間を要するため、秘匿データの入出力命令に要する時間は、通常データの入出力命令に要する時間に比べて長くなる。たとえば、秘匿データをストレージデバイス 2 0 0 から読み出すとき、ストレージデバイス 2 0 0 に対して読出命令を発行すると、ストレージデバイス 2 0 0 は、自身の暗号エンジンにより該当する秘匿データを機密データ記憶領域から読み出し、その秘匿データをホスト装置に送出するために用いる暗号鍵をホスト装置との間でやり取りし

た後、その秘匿データを暗号鍵で暗号化してからバスに出力する。このとき、暗号化および復号などの処理を実行している間は、バスは実際には使われていないにもかかわらず、この命令により占有された状態にある。

【0018】

本実施の形態では、このような無駄なバスの占有を極力省き、バスを効率良く利用して処理の高速化を図るために、秘匿データの入出力のための一連の暗号入出力処理を複数の手順に分割し、命令を細分化して発行する。そして、暗号化または復号など、バスを使わない処理が行われている間は、できる限りバスを開放して他の命令が発行できるようにする。

【0019】

ところが、秘匿データを入出力するための暗号入出力処理を複数の手順に分割したとき、それらの手順の実行順序が前後すると、セキュリティホールが発生する恐れがある。そのため、本実施の形態では、ストレージデバイス200の暗号エンジンは、秘匿データの入出力における手順の実行順序を管理し、不正な順序の命令を受信した場合、その命令の実行を拒否し、エラー応答を返す。

【0020】

記録装置100や再生装置300などのホスト装置がストレージデバイス200に対して暗号入出力処理に関する命令を発行し、つづいて、その次の順序の命令を発行したとき、ストレージデバイス200側が前の命令を実行中の場合は、次の命令は受理されない。ホスト装置が、次の命令を受理されるまで、闇雲にストレージデバイス200に命令を発行し続けるのは効率的でない。そのため、本実施の形態では、ホスト装置は予めストレージデバイス200から命令の実行に要する時間を推定するための情報を取得し、命令を発行した後、その命令の実行に要すると推定される時間だけ待機した後、次の命令を発行する。これにより、無駄な命令の発行を最小限に抑えることができる。

【0021】

以下、秘匿データの入出力の例として、画像や音楽などのデジタルコンテンツを記録再生する場合について説明する。コンテンツ自身を秘匿データとして扱ってもよいが、本実施の形態では、コンテンツを暗号化し、暗号化されたコンテン

ツ自身は通常のデータとして入出力を行う。そして、暗号化されたコンテンツを復号するための鍵（コンテンツ鍵と呼ぶ）を含む、コンテンツの復号および利用に必要なデータ（ライセンスデータと呼ぶ）を、秘匿データとして上述のセキュア機能を用いて入出力を行う。これにより、十分な耐タンパ性を維持しつつ、データの入出力を簡略化し、処理の高速化および消費電力の低減を図ることができる。ここで、ライセンスデータは、コンテンツ鍵の他に、ライセンスの利用、移動、複製に関する情報や、ライセンスデータを特定するためのライセンスIDなどを含む。以下、記録装置100、再生装置300などのホスト装置がストレージデバイス200に対して発行する命令のうち、セキュア機能のための命令を「セキュアコマンド」とも呼び、その他の命令を「通常コマンド」とも呼ぶ。

【0022】

図2は、実施の形態に係る記録装置100の内部構成を示す。この構成は、ハードウェア的には、任意のコンピュータのCPU、メモリ、その他のLSIなどで実現でき、ソフトウェア的にはメモリにロードされた記録制御機能のあるプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できることは、当業者には理解されるところである。記録装置100は、主に、コントローラ101、ストレージインタフェース102、暗号エンジン103、暗号器104、コンテンツエンコーダ105、およびそれらを電氣的に接続するデータバス110を備える。

【0023】

コンテンツエンコーダ105は、オンラインまたはオフラインにより取得したコンテンツを所定の形式にエンコードする。たとえば、ネットワークを介して取得した画像データをJPEG形式にエンコードしてもよいし、放送波から取得した映像データをMPEG形式にエンコードしてもよい。暗号器104は、エンコードされたコンテンツを暗号化し、暗号化されたコンテンツを復号するためのコンテンツ鍵を発行する。暗号化されたコンテンツは、データバス110およびストレージインタフェース102を介してストレージデバイス200に記録される

。コンテンツ鍵は、暗号エンジン 103 に通知され、暗号エンジン 103 を介してストレージデバイス 200 に記録される。暗号エンジン 103 は、コンテンツ鍵を含むライセンスデータをストレージデバイス 200 に入力するために、ストレージデバイス 200 との間で暗号通信の制御を行う。ストレージインタフェース 102 は、ストレージデバイス 200 とのデータの入出力を制御する。コントローラ 101 は、記録装置 100 の構成要素を統括的に制御する。

【0024】

図 3 は、実施の形態に係る再生装置 300 の内部構成を示す。これらの機能ブロックも、ハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できる。再生装置 300 は、主に、コントローラ 301、ストレージインタフェース 302、暗号エンジン 303、復号器 304、コンテンツデコーダ 305、およびそれらを電氣的に接続するデータバス 310 を備える。

【0025】

ストレージインタフェース 302 は、ストレージデバイス 200 とのデータの入出力を制御する。暗号エンジン 303 は、コンテンツ鍵を含むライセンスデータをストレージデバイス 200 から受信するために、ストレージデバイス 200 との間で暗号通信の制御を行う。復号器 304 は、ストレージデバイス 200 から読み出した暗号化されたコンテンツを、ストレージデバイス 200 から入手したライセンスデータに含まれるコンテンツ鍵により復号する。コンテンツデコーダ 305 は、復号器 304 により復号されたコンテンツをデコードして出力する。たとえば、画像データであれば、図示しない表示装置に出力し、音声データであれば、図示しないスピーカに出力する。コントローラ 301 は、再生装置 300 の構成要素を統括的に制御する。

【0026】

図 4 は、実施の形態に係るストレージデバイス 200 の内部構成を示す。ストレージデバイス 200 は、主に、コントローラ 201、ストレージインタフェース 202、暗号エンジン 203、通常データ記憶部 204、機密データ記憶部 205、およびそれらを電氣的に接続するデータバス 210 を備える。

【0 0 2 7】

ストレージインタフェース 2 0 2 は、記録装置 1 0 0 および再生装置 3 0 0 とのデータの入出力を制御する。暗号エンジン 2 0 3 は、コンテンツ鍵を含むライセンスデータなどの秘匿データを記録装置 1 0 0 および再生装置 3 0 0 との間で入出力するための暗号通信の制御を行う。通常データ記憶部 2 0 4 は、暗号化されたコンテンツや通常のデータなどを記録する。機密データ記憶部 2 0 5 は、コンテンツ鍵を含むライセンスデータなどの秘匿データを記録する。コントローラ 2 0 1 は、ストレージデバイス 2 0 0 の構成要素を統括的に制御する。通常データ記憶部 2 0 4 は、外部から直接アクセス（データの入出力）が行われるが、機密データ記憶部 2 0 5 は、暗号エンジン 2 0 3 を介しないとアクセス（データの入出力）ができないように構成される。

【0 0 2 8】

図 5 は、図 2 に示した記録装置 1 0 0 の暗号エンジン 1 0 3 の内部構成を示す。暗号エンジン 1 0 3 は、認証部 1 2 0、第 1 暗号部 1 2 1、乱数発生部 1 2 2、復号部 1 2 3、第 2 暗号部 1 2 4、ログメモリ 1 2 5、およびこれらの構成要素の少なくとも一部を電氣的に接続するローカルバス 1 3 0 を備える。

【0 0 2 9】

認証部 1 2 0 は、ストレージデバイス 2 0 0 から取得した証明書を認証する。証明書は、公開鍵を含む平文の情報（「証明書本体」と呼ぶ）と、証明書本体に対して付される電子署名からなる。この電子署名は、証明書本体に対してハッシュ関数による演算（この演算処理を「ハッシュ演算」と呼ぶ）を施した結果を、第三者機関である認証局（図示せず）のルート鍵 K_{pa} によって暗号化したデータである。ルート鍵 K_{pa} は、認証局によって厳重に管理されている非公開な鍵であり、認証局の秘密鍵となる。認証部 1 2 0 は、このルート鍵 K_{pa} と対をなす認証鍵 K_Pa を保持している。この認証鍵 K_Pa は証明書の正当性を検証する公開鍵である。証明書の正当性の検証は、検証すべき証明書の証明書本体に対するハッシュ関数の演算結果と、認証鍵 K_Pa で電子署名を復号した結果を比較する処理であり、両者が一致したとき、正当であると判断する。この証明書の正当性を判断し、正当な証明書を承認する処理を認証と呼ぶ。認証部 1 2 0 は、認証

に成功すると、ストレージデバイス 200 の公開鍵 KP_c を取り出して第 1 暗号部 121 に伝達し、認証に失敗すると、エラー通知を出力する。

【0030】

乱数発生部 122 は、ストレージデバイス 200 との間で暗号通信を行うために一時的に使用されるチャレンジ鍵 Ks_1 を発生する。暗号通信を行う度に、乱数によりチャレンジ鍵 Ks_1 を生成することで、チャレンジ鍵 Ks_1 を見破られる可能性を最小限に抑えることができる。生成されたチャレンジ鍵 Ks_1 は、第 1 暗号部 121 および復号部 123 に伝達される。第 1 暗号部 121 は、ストレージデバイス 200 にチャレンジ鍵 Ks_1 を通知するために、認証部 120 により取り出されたストレージデバイス 200 の公開鍵 KP_c でチャレンジ鍵 Ks_1 を暗号化して、暗号化共通鍵 $E(KP_c, Ks_1)$ を生成する。ここで、関数 E は暗号化を示し、 $E(KP_c, Ks_1)$ は、 KP_c で Ks_1 を暗号化したものであることを示す。

【0031】

復号部 123 は、チャレンジ鍵 Ks_1 で暗号化されたデータを復号する。ストレージデバイス 200 で発行されたセッション鍵 Ks_2 は、チャレンジ鍵 Ks_1 により暗号化されてストレージデバイス 200 から供給されるため、復号部 123 は、乱数発生部 122 が発生したチャレンジ鍵 Ks_1 を取得して、セッション鍵 Ks_2 を復号する。復号したセッション鍵 Ks_2 は第 2 暗号部 124 に伝達される。第 2 暗号部 124 は、暗号器 104 がコンテンツを暗号化する際に発行したコンテンツ鍵を含むライセンスデータを取得し、そのライセンスデータをストレージデバイス 200 で発行されたセッション鍵 Ks_2 により暗号化する。ログメモリ 125 は、一連の暗号入出力処理におけるトランザクションログを保持する。

【0032】

図 5 では、暗号エンジン 103 の構成要素のうち、認証部 120、第 1 暗号部 121、復号部 123、第 2 暗号部 124、およびログメモリ 125 がローカルバス 130 により電氣的に接続されており、ローカルバス 130 を介して記録装置 100 のデータバス 110 に接続されている。各構成要素を接続する形態には

いろいろな変更例が考えられるが、本実施の形態では、チャレンジ鍵を発生する乱数発生部 1 2 2 が、直接データバス 1 1 0 に接続されないよう配慮している。これにより、暗号エンジン 1 0 3 内で使用される各鍵が、記録装置 1 0 0 の他の構成要素などを介して外部に漏洩することを防ぎ、セキュリティ性を向上させることができる。

【 0 0 3 3 】

図 6 は、図 3 に示した再生装置 3 0 0 の暗号エンジン 3 0 3 の内部構成を示す。暗号エンジン 3 0 3 は、証明書出力部 3 2 0、第 1 復号部 3 2 1、暗号部 3 2 2、乱数発生部 3 2 3、第 2 復号部 3 2 4、およびこれらの構成要素の少なくとも一部を電氣的に接続するローカルバス 3 3 0 を備える。

【 0 0 3 4 】

証明書出力部 3 2 0 は、再生装置 3 0 0 の証明書を出力する。証明書は、証明書出力部 3 2 0 が保持してもよいし、図示しない証明書保持部に保持しておき、それを読み出してもよい。証明書は、再生装置 3 0 0 の公開鍵 K P b を含む証明書本体と、証明書本体に対して付される電子署名からなる。電子署名は、ストレージデバイス 2 0 0 の証明書と同様に、認証局のルート鍵 K p a により暗号化される。第 1 復号部 3 2 1 は、公開鍵 K P b によって暗号化されたデータを秘密鍵 K p b で復号する。ストレージデバイス 2 0 0 で発行されたチャレンジ鍵 K s 3 は、再生装置 3 0 0 の公開鍵 K P b により暗号化されてストレージデバイス 2 0 0 から供給されるため、第 1 復号部 3 2 1 は、自身の秘密鍵 K p b により復号してチャレンジ鍵 K s 3 を取り出す。取り出されたチャレンジ鍵 K s 3 は、暗号部 3 2 2 に伝達される。乱数発生部 3 2 3 は、ストレージデバイス 2 0 0 との間で暗号通信を行うために一時的に使用されるセッション鍵 K s 4 を発生する。生成されたセッション鍵 K s 4 は、暗号部 3 2 2 および第 2 復号部 3 2 4 に伝達される。

【 0 0 3 5 】

暗号部 3 2 2 は、ストレージデバイス 2 0 0 にセッション鍵 K s 4 を通知するために、復号部 3 2 1 により取り出されたチャレンジ鍵 K s 3 でセッション鍵 K s 4 を暗号化する。第 2 復号部 3 2 4 は、セッション鍵 K s 4 で暗号化されたデ

ータを復号する。ライセンスデータは、セッション鍵 $K_s 4$ により暗号化されてストレージデバイス 200 から供給されるため、第2復号部 324 は、乱数発生部 323 が発生したセッション鍵 $K_s 4$ により復号して、ライセンスデータを取り出す。取り出されたライセンスデータは、復号器 304 に伝達され、復号器 304 はこのライセンスデータに含まれるコンテンツ鍵を用いて暗号化されたコンテンツを復号する。

【0036】

図6に示した暗号エンジン 303 においても、各構成要素を接続する形態にはいろいろな変更例が考えられるが、本実施の形態では、チャレンジ鍵を発生する乱数発生部 323 が直接データバス 310 に接続されないように構成することで、暗号エンジン 303 内で使用される暗号鍵が外部に漏洩することを防ぐ。

【0037】

図7は、図4に示したストレージデバイス 200 の暗号エンジン 203 の内部構成を示す。これらの機能ブロックも、ハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できる。暗号エンジン 203 は、データレジスタ 220、状態レジスタ 221、制御部 222、乱数発生部 224、証明書出力部 225、認証部 226、第1復号部 227、第1暗号部 228、第2復号部 229、第2暗号部 230、ログメモリ 231、およびこれらの構成要素の少なくとも一部を電氣的に接続するローカルバス 240 を備える。

【0038】

データレジスタ 220 は、データ入出力用のレジスタであり、暗号エンジン 203 の外部の構成との間でデータの入出力を仲介する。状態レジスタ 221 は、コントローラ 201 が記録装置 100 または再生装置 300 から受信したセキュアコマンドの実行を暗号エンジン 203 に指示するための実行指示と、暗号エンジン 203 がセキュアコマンドの処理状態または処理結果などをコントローラ 201 に通知するためのステータス情報などを保持する。

【0039】

ストレージデバイス 200 のコントローラ 201 が、記録装置 100 または再生装置 300 のコントローラからセキュアコマンドを受信すると、状態レジスタ

221にその命令の実行指示（開始指示）を格納する。たとえば、セキュアコマンドのそれぞれに実行順に番号を付しておき、コントローラ201が受信したセキュアコマンドの番号を状態レジスタ221に格納することで、暗号エンジン203に対してそのコマンドの実行を指示する。制御部222は、状態レジスタ221に新しい実行指示が格納されると、その処理を開始する。

【0040】

制御部222は、コントローラ201から通知された命令の処理状態および処理結果を状態レジスタ221に格納する。処理状態は、たとえば、処理が実行されている状態を示す「Busy」、処理が実行されていない状態を示す「Ready」の2つのステータスで表現することができ、処理結果は、たとえば、処理が正常に終了したことを示す「Normal」、処理が異常終了したことを示す「Error」の2つのステータスで表現することができる。制御部222は、暗号エンジン203によりセキュアコマンドの実行が開始されると、状態レジスタ221の処理状態を「Busy」に変更し、セキュアコマンドの実行が終了すると、状態レジスタ221の処理状態を「Ready」に変更するとともに、その命令の終了理由を処理結果に反映させる。

【0041】

乱数発生部224は、記録装置100または再生装置300との間の暗号通信に一時的に使用されるセッション鍵Ks2またはチャレンジ鍵Ks3を発生する。このとき乱数発生部224は乱数演算を行う。ログメモリ231は、一連の暗号入出力処理におけるトランザクションログを保持する。

【0042】

証明書出力部225は、ストレージデバイス200の証明書を出力する。証明書は、証明書出力部225が保持してもよいし、ストレージデバイス200の所定の記憶領域、たとえば機密データ記憶部205に保持しておき、それを読み出してもよい。証明書は、ストレージデバイス200の公開鍵Kpcを含む証明書本体と、証明書本体に付された電子署名とを含む。電子署名は、認証局のルート鍵Kpaにより暗号化される。認証部226は、再生装置300から取得した証明書を認証する。認証部226は、外部から提供された証明書の正当性を認証鍵

K P aにより検証する。認証部 226 は、認証に成功すると、証明書に含まれる再生装置 300 の公開鍵 K P b を取り出してデータレジスタ 220 に格納し、認証に失敗すると、制御部 222 へエラー通知を出力する。認証部 226 は、証明書を認証する際、公開鍵暗号方式の公開鍵で暗号化されたデータを復号する復号演算、および証明書本体に対するハッシュ演算を行う。

【0043】

第1復号部 227 は、公開鍵暗号方式の公開鍵で暗号化されたデータを復号するための復号演算を行う。具体的には、自身の公開鍵 K P c で暗号化されたデータを、自身の秘密鍵 K p c で復号する。第1暗号部 228 は、公開鍵暗号方式の公開鍵でデータを暗号化するための暗号化演算を行う。具体的には、再生装置 300 から受け取った再生装置 300 の公開鍵 K P b で、乱数発生部 224 が発行したチャレンジ鍵 K s 3 を暗号化する。第2復号部 229 は、共通鍵暗号方式の鍵で暗号化されたデータを復号するための復号演算を行う。具体的には、乱数発生部 224 が発行したセッション鍵 K s 2 またはチャレンジ鍵 K s 3 で暗号化されたデータを、それぞれセッション鍵 K s 2 またはチャレンジ鍵 K s 3 で復号する。第2暗号部 230 は、共通鍵暗号方式の鍵でデータを暗号化するための暗号化演算を行う。具体的には、記録装置 100 が発行したチャレンジ鍵 K s 1 または再生装置 300 が発行したセッション鍵 K s 4 で、乱数発生部 224 が発行されたセッション鍵 K s 2 またはライセンスデータをそれぞれ暗号化する。

【0044】

図8は、ホスト装置が、ストレージデバイスがセキュアコマンドセットをサポートしているか否かを示す情報、さらに、セキュアコマンドに対応している場合、セキュアコマンドの実行に必要な時間を推定するための情報をストレージデバイスから取得するイニシャル手順を示す。ストレージデバイス 200 が記録装置 100 に接続されると、記録装置 100 のコントローラ 101 は、ストレージデバイス 200 にデバイス情報出力命令を発行する (S400)。ストレージデバイス 200 のコントローラ 201 は、記録装置 100 のコントローラ 101 からデバイス情報出力命令を受信すると (S402)、デバイス情報を出力する (S404)。デバイス情報として、たとえば、ハードディスクの種類、通常データ

の記録容量、インタフェースの条件、サポートするコマンドセットなどの情報が通知される。コントローラ101は、ストレージデバイス200のデバイス情報を受信すると(S406)、ストレージデバイス200がセキュアコマンドセットをサポートしているか否かを判断し(S408)、サポートしていなければ(S408のN)、セキュアコマンド非対応のハードディスクとして取り扱う。

【0045】

ストレージデバイス200がセキュアコマンドをサポートしていれば(S408のY)、つづいて、コントローラ101は、セキュア情報出力命令を発行する(S410)。コントローラ201は、セキュア情報出力命令を受信すると(S412)、セキュア情報を出力する(S414)。セキュア情報として、ストレージデバイス200がセキュアコマンドを受信したときに、その命令を実行するのに要する時間を推定するための情報、たとえば、セキュアコマンド命令を実行するために用いられる基本処理、すなわち、公開鍵方式暗号化演算、共通鍵方式暗号化演算、公開鍵方式復号演算、共通鍵方式復号演算、ハッシュ演算、乱数発生演算、ログ検索処理、などの個々の基本処理に要する典型的な時間(Typical time)が通知される。典型的な時間とは、たとえば、同一のセキュアコマンドを100回発行すると、そのうち99回はその時間内に終了するといった、例外を除く処理時間を意味する。コントローラ101は、ストレージデバイス200のセキュア情報を受信すると(S416)、受信した情報をもとに各セキュアコマンドを発行したときの待ち時間を決定する(S418)。

【0046】

命令を実行するのに要する時間を推定するための情報として、各基本処理に要する典型的な処理時間に代えて、平均処理時間または最大処理時間を出力するようにしても良いし、これらを組み合わせて出力するようにしてもよい。いずれにしても、コントローラ101は、ストレージデバイス200が出力した基本処理に要する処理時間を取得し、各セキュアコマンドが実行する基本処理に基づいて、各セキュアコマンドに要する時間を推定する。また、基本処理に要する処理時間に代えて、各セキュアコマンドの実行に要する典型的な処理時間、平均処理時間または最大処理時間を出力するようにしても良いし、これらを組み合わせて出

力するようにしてもよい。いずれにしても、コントローラ101は、ストレージデバイス200が出力した推定するための情報から、各セキュアコマンドの発行後に次のセキュアコマンドを発行するまでの待ち時間を推定する。図8では、記録装置100がホスト装置として機能する例について説明したが、再生装置300がホスト装置として機能する場合も同様である。

【0047】

図9、図10、および図11は、記録装置100がストレージデバイス200にライセンスデータを記録するまでの手順を示す。まず、記録装置100のコントローラ101は、ストレージデバイス200に対して証明書出力命令を発行する(S102)。コントローラ201は、証明書出力命令を正常に受理すると、暗号エンジン203に証明書の出力を命じる。セキュアコマンドの発行と受理の詳細については図16において詳述する。制御部222は、状態レジスタ221の処理状態を「B u s y」に変更し(S300)、証明書出力部225は証明書をデータレジスタ220に格納する(S302)。処理が終了すると、制御部222は状態レジスタ221の処理状態を「R e a d y」、処理結果を「N o r m a l」に変更する(S304)。コントローラ201は、データレジスタ220から証明書を読み出して記録装置100へ出力する(S106)。

【0048】

コントローラ101は、ストレージデバイス200から証明書を取得すると、それを記録装置100の暗号エンジン103に送る(S108)。暗号エンジン103がストレージデバイス200の証明書を受信すると(S110)、認証部120は、認証鍵K P aで証明書の正当性を認証する(S112)。証明書の正当性が承認されなかった場合は(S112のN)、認証部120はエラー通知をコントローラ101に送信する(S190)。コントローラ101は、エラー通知を受信すると(S192)、処理を異常終了する。証明書が認証された場合は(S112のY)、暗号エンジン103は、乱数発生部122によりチャレンジ鍵K s 1を発生し(S114)、生成したチャレンジ鍵K s 1を暗号部121によりストレージデバイス200の公開鍵K P cで暗号化して暗号化共通鍵E (K P c、K s 1)を生成し、コントローラ101へ送る(S116)。

【0049】

コントローラ101は、暗号化共通鍵E (K P c、K s 1)を受信すると(S118)、ストレージデバイス200に対してチャレンジ鍵入力命令を発行する(S120)。コントローラ201は、チャレンジ鍵入力命令を正常に受理すると、暗号化共通鍵E (K P c、K s 1)の入力要求を記録装置100へ出力する(S122)。コントローラ101は、この入力要求に応じて、暗号化共通鍵E (K P c、K s 1)をストレージデバイス200へ出力する(S124)。コントローラ201は、暗号化共通鍵E (K P c、K s 1)を受理すると(S126)、それをデータレジスタ220に格納し(S128)、受理通知をコントローラ101に返す(S130)。そして、チャレンジ鍵の受理を暗号エンジン203に命じる。

【0050】

制御部222は、状態レジスタ221の処理状態を「B u s y」に変更し(S310)、データレジスタ220より暗号化共通鍵(K P c、K s 1)を取り出し、第1復号部227に与える。第1復号部227は、ストレージデバイス200の秘密鍵K p cで与えられた暗号化共通鍵E (K P c、K s 1)を復号してチャレンジ鍵K s 1を取り出し(S312)、制御部222に出力する(S314)。制御部222は、チャレンジ鍵K s 1を取得すると、状態レジスタ221の処理状態を「R e a d y」、処理結果を「N o r m a l」に変更する(S316)。

【0051】

一方、コントローラ101は、暗号化共通鍵E (K P c、K s 1)の入力を終了すると、ストレージデバイス200がチャレンジ鍵入力命令の実行に要すると推定される時間待機する(S131)。チャレンジ鍵入力命令で実行される処理は、暗号化共通鍵E (K P c、K s 1)を復号して共通鍵K s 1を取り出し、それを保持する処理であるから、公開鍵方式の復号処理に要する時間だけ待機すればよい。この間は、通常コマンドの発行が可能となり、コントローラ101は必要に応じて通常コマンドを発行する。チャレンジ鍵入力命令の実行に要すると推定される時間が経過すると、コントローラ101は、ストレージデバイス200

に対してセッション鍵準備命令を発行する（S132）。後述するように、チャレンジ鍵入力命令の実行が終了していなければ、コントローラ201はセッション鍵準備命令を受理しないが、命令の実行が終了していれば、コントローラ201はセッション鍵準備命令を受理する。

【0052】

コントローラ201は、セッション鍵準備命令を正常に受理すると、ライセンスIDの入力要求を記録装置100へ出力する（S133）。このライセンスIDは、図9から図11に示される一連の暗号入出力処理によってストレージデバイス200へ書き込まれるライセンスデータのIDであり、トランザクションログの記録、入力されたライセンスデータの確認のために用いられる。コントローラ101は、この入力要求に応じて、ライセンスIDをストレージデバイス200へ出力する（S134）。コントローラ201は、ライセンスIDを受理すると（S136）、それをデータレジスタ220に格納し（S138）、受理通知をコントローラ101に返す（S140）。

【0053】

制御部222は、状態レジスタ221の処理状態を「B u s y」に変更する（S320）。乱数発生部224は、セッション鍵Ks2を発生し、制御部222に出力する（S322）。そして、制御部222は、ログメモリ231にトランザクションログとしてライセンスID、生成したセッション鍵Ks2およびステータス情報としてRP（Receive Prepare/受信準備）を記録し（S326）、セッション鍵Ks2およびチャレンジ鍵Ks1を第2暗号部230に与える。第2暗号部230は、セッション鍵Ks2をチャレンジ鍵Ks1で暗号化して暗号化鍵E（Ks1、Ks2）を生成し、データレジスタ220に格納する（S328）。処理が終了すると、制御部222は状態レジスタ221の処理状態を「R e a d y」、処理結果を「N o r m a l」に変更する（S329）。

【0054】

一方、コントローラ101は、セッション鍵準備命令の受理通知を受け取ると、ストレージデバイス200がセッション鍵準備命令の実行に要すると推定される時間待機する（S141）。セッション鍵準備命令で実行される処理は、セッ

セッション鍵 $Ks2$ を発生し、 $Ks1$ で $Ks2$ 暗号化する処理であるから、乱数発生処理と共通鍵方式の暗号化処理に要する時間だけ待機すればよい。セッション鍵準備命令の実行に要すると推定される時間が経過すると、コントローラ 101 はストレージデバイス 200 に対してセッション鍵出力命令を発行し、コントローラ 201 はセッション鍵出力命令を受理する (S142)。後述するように、セッション鍵準備命令の実行が終了していなければ、セッション鍵出力命令は受理されないが、命令の実行が終了していれば、受理される。命令を受理すると、コントローラ 201 は、暗号化鍵 $E(Ks1, Ks2)$ をデータレジスタ 220 から読み出してコントローラ 101 へ出力する (S146)。

【0055】

コントローラ 101 は、ストレージデバイス 200 から暗号化鍵 $E(Ks1, Ks2)$ を受信すると、それを暗号エンジン 103 に送る (S148)。暗号エンジン 103 がコントローラ 101 から暗号化鍵 $E(Ks1, Ks2)$ を受信すると (S150)、復号部 123 は、チャレンジ鍵 $Ks1$ で暗号化鍵 $E(Ks1, Ks2)$ を復号してセッション鍵 $Ks2$ を取り出す (S152)。つづいて、暗号エンジン 103 は、第2暗号部 124 により、暗号器 104 が発行したコンテンツのコンテンツ鍵とライセンス ID を含むライセンスデータをストレージデバイス 200 が発行したセッション鍵 $Ks2$ で暗号化して暗号化ライセンスデータを生成し、コントローラ 101 に送る (S154)。

【0056】

コントローラ 101 は、暗号化ライセンスデータを受信すると (S156)、ストレージデバイス 200 に対してライセンスデータ入力命令を発行する (S158)。ライセンス入力命令はストレージデバイス 200 に対してライセンスデータを書き込むアドレスの指定を伴っている。コントローラ 201 がライセンスデータ入力命令を正常に受理すると、コントローラ 201 は、暗号化ライセンスデータの入力要求を記録装置 100 へ出力する (S160)。コントローラ 101 は、データの入力要求に応え、暗号化ライセンスデータをストレージデバイス 200 へ出力する (S162)。コントローラ 201 は、暗号化ライセンスデータを受理すると (S164)、それをデータレジスタ 220 に格納する (S166)。

）。そして、データの受理通知を記録装置100へ出力し、同時に、ライセンスデータを受理するように暗号エンジン203へ命じる（S167）。

【0057】

制御部222は、状態レジスタ221の処理状態を「B u s y」に変更し（S330）、データレジスタ220から暗号化ライセンスデータを取得して、セッション鍵Ks2と共に第2復号部229へ与える。第2復号部229は、セッション鍵Ks2で暗号化ライセンスデータを復号し、ライセンスデータを取り出し、取り出したライセンスデータを制御部222に提供する（S332）。制御部222は、ライセンスデータを受け取ると、ライセンスデータ内のライセンスIDとトランザクションログ内のライセンスIDとの比較を行う（S334）。2つのライセンスIDが異なった場合（S334のN）、制御部222は、状態レジスタ221の処理状態を「R e a d y」、処理結果を「E r r o r」に変更する（S336）。

【0058】

2つのライセンスIDが一致した場合（S334のY）、制御部222は、トランザクションログに指定アドレスを記録し、トランザクションログ内のステータス情報をRPからRL（Receive License／ライセンス受理）へ変更する（S338）。そして、ライセンスデータを機密データ記憶部205の指定アドレスに記憶する格納処理を行う（S340）。データの記憶が何らかの理由で正常に終了しないとライセンスデータが失われるので、格納処理が正常に終了したか否かの確認を行う（S342）。データが記録されずに格納処理が終了した場合（S342のN）、制御部222は、状態レジスタ221の処理状態を「R e a d y」、処理結果を「E r r o r」に変更する（S344）。データが正常に記憶されている場合（S342のY）、ログメモリ231のトランザクションログ内のステータス情報をRLからRC（Receive Completed／受信完了）へ変更する（S346）。トランザクションログの変更が終了すると、制御部222は、状態レジスタ221の処理状態を「R e a d y」、処理結果を「N o r m a l」に変更する（S348）。

【0059】

一方、コントローラ 101 は、データの受理通知を受信すると、ストレージデバイス 200 がライセンスデータ入力命令の実行に要すると推定される時間待機する (S168)。ライセンスデータ入力命令で実行される処理は、暗号化ライセンスデータをセッション鍵 K_s 2 で復号する処理と、入力したライセンスデータを機密データ記憶部 205 に記録する処理であるから、共通鍵方式の復号処理に要する時間と記録に要する時間を加算した時間だけ待機すればよい。ライセンスデータ入力命令の実行に要すると推定される時間が経過すると、コントローラ 101 はストレージデバイス 200 に対してライセンスデータの記憶を確認するために終了確認命令を発行し、ライセンスデータ入力命令の実行が終了していれば、コントローラ 201 は終了確認命令を受信する (S170)。制御部 222 は、状態レジスタ 221 の処理結果を参照して、先の命令、すなわちライセンスデータ入力命令の処理結果をコントローラ 101 に返す (S172)。コントローラ 101 は、コントローラ 201 からライセンス入力命令の処理結果を受信すると (S174)、受信した処理結果を参照してライセンス入力命令が正常終了したか否かを確認する (S176)。ライセンスデータがストレージデバイス 200 に記憶された場合は (S176 の Y)、コントローラ 101 は処理を正常に終了する。一方、記憶に失敗した場合は (S176 の N)、コントローラ 101 は処理を異常終了する。このとき、コントローラ 101 は、ライセンスデータの記録を再度試みることとなる。

【0060】

以上の手順により、コンテンツを復号するためのライセンスデータがストレージデバイス 200 に記録される。暗号化コンテンツは、通常データであるため通常コマンドによって直接ストレージデバイス 200 の通常コマンドによって書き込まれるため、ここでは説明を省略する。

【0061】

図 12 は、電源投入後、ストレージデバイス 200 にライセンスデータを記憶するまでの ATA インタフェース上の一連の手順を示すシーケンス図である。図 8 に示したイニシャル手順と、図 9 から図 11 に示した記録装置 100 がストレージデバイス 200 にライセンスデータを記録するまでの手順が、正常に処理が

推移した場合の例である。

【0062】

「Host ATA-IF」は、記録装置100のストレージインタフェース102に、「Storage ATA-IF」は、ストレージデバイス200のストレージインタフェース202に相当する。2つのATA-IFに挟まれた中央部分には、セキュアコマンドが記載されている。コマンド名の後ろに記載されている(W)、(R)、(S)はコマンドの特性を示すもので、(W)はデータ列の入力を伴うコマンド、すなわち、命令受理後ストレージデバイス200からデータ要求があるコマンドであることを示し、(R)は、逆にデータ列の出力を伴うコマンド、(S)は、データ列の入出力を伴わないコマンドであることを示す。

【0063】

また、コマンド「IDENTIFY_DEVICE」、「GET_SECURITY_FEATURE」、「GET_CERTIFICATE」、「PUT_CHALLENGE_KEY」、「CREATE_SESSION_KEY」、「GET_SESSION_KEY」、「PUT_LICENSE」、「GET_COMPLETION_STATUS」は、それぞれデバイス情報出力命令、セキュア情報出力命令、証明書出力命令、チャレンジ鍵入力命令、セッション鍵準備命令、チャレンジ鍵出力命令、ライセンス入力命令、終了確認命令に相当する。また、11は、S110、S112、S114、S116の処理、12は、S150、S152、S154の処理および記録装置100におけるログ記録処理、21は、S128、S312の処理、22は、S138、S322、S326、S328の処理、23は、S172、S332、S334、S338、S340、S346の処理に対応し、図12では、内部の詳細な処理は示されていない。

【0064】

このシーケンスは、ストレージデバイス200の情報を取得する「Initialization STEP (イニシャル手順)」、チャレンジ鍵Ks1をストレージデバイス200が取得するまでの「Authentication S

TEP」、およびライセンスを転送して書き込むまでの「Transmission STEP」に区分される。「Transmission STEP」終了後、「Transmission STEP」の先頭へ戻る矢印は、ライセンスデータを続けてストレージデバイス200に記憶する場合、「Initialization STEP」および「Authentication STEP」を共有しても良いことを示す。「Initialization STEP」および「Authentication STEP」を省略することによりライセンスデータに対する安全性が低下することはない。また、「Transmission STEP」終了後、「Authentication STEP」の先頭へ戻る矢印は、すべての手順において「Initialization STEP」を共通して良いことを示す。

【0065】

図13、図14、および図15は、再生装置300がストレージデバイス200からライセンスデータを読み出すまでの手順を示す。まず、再生装置300の暗号エンジン303は、証明書出力部320により、証明書をコントローラ301へ送る(S202)。コントローラ301は、暗号エンジン303から証明書を受信すると(S204)、ストレージデバイス200に対して証明書入力命令を発行する(S206)。コントローラ201は、証明書入力命令を正常に受理すると、証明書の入力要求をコントローラ301に出力する(S208)。コントローラ301は、この入力要求に応じて、コントローラ201に証明書を出力する(S210)。コントローラ201は、証明書を受信すると(S212)、それをデータレジスタ220に格納し(S213)、受理通知をコントローラ301に返す(S214)。

【0066】

制御部222は、状態レジスタ221の処理状態を「Busy」に変更し(S400)、認証部226は、認証鍵KPaで証明書の正当性を検証する(S402)。証明書の正当性が承認されなかった場合は(S402のN)、認証部402はエラー通知を出力し(S408)、コントローラ201は、そのエラー通知をコントローラ301に出力する(S290)。コントローラ301は、エラー

通知を受信すると (S 2 9 2)、処理を異常終了する。証明書の正当性が承認された場合は (S 4 0 2 の Y)、認証部 2 2 6 は、証明書から取り出された公開鍵 K P b をデータレジスタ 2 2 0 に格納し (S 4 0 4)、制御部 2 2 2 は、状態レジスタ 2 2 1 の処理状態を「R e a d y」に、処理結果を「N o r m a l」に変更する (S 4 0 6)。

【0067】

一方、コントローラ 3 0 1 は、証明書の受理通知を受け取ると、ストレージデバイス 2 0 0 が証明書入力命令の実行に要すると推定される時間待機する (S 2 1 6)。証明書入力命令の実行に要すると推定される時間が経過すると、コントローラ 3 0 1 は、ストレージデバイス 2 0 0 に対してチャレンジ鍵準備命令を発行する (S 2 1 8)。コントローラ 2 0 1 がチャレンジ鍵準備命令を受理すると、チャレンジ鍵準備命令の受理通知をコントローラ 3 0 1 に返す (S 2 2 0)。制御部 2 2 2 は、状態レジスタ 2 2 1 の処理状態を「B u s y」に変更し (S 4 1 0)、乱数発生部 2 2 4 は、チャレンジ鍵 K s 3 を発生し (S 4 1 2)、第 1 暗号部 2 2 8 は、公開鍵 K P b でチャレンジ鍵 K s 3 を暗号化して暗号化鍵 E (K P b、K s 3) を生成し、データレジスタ 2 2 0 に一時格納する (S 4 1 4)。処理が終了すると、制御部 2 2 2 は、状態レジスタ 2 2 1 の処理状態を「R e a d y」に、処理結果を「N o r m a l」に変更する (S 4 1 6)。

【0068】

一方、コントローラ 3 0 1 は、チャレンジ鍵準備命令の受理通知を受け取ると、ストレージデバイス 2 0 0 がチャレンジ鍵準備命令の実行に要すると推定される時間待機する (S 2 2 2)。チャレンジ鍵準備命令の実行に要すると推定される時間が経過すると、コントローラ 3 0 1 は、ストレージデバイス 2 0 0 に対してチャレンジ鍵出力命令を発行する (S 2 2 4)。コントローラ 2 0 1 は、チャレンジ鍵出力命令を受理すると、暗号化鍵 E (K P b、K s 3) をデータレジスタ 2 2 0 から読み出してコントローラ 3 0 1 に送信する (S 2 2 6)。

【0069】

コントローラ 3 0 1 は、暗号化共通鍵 E (K P b、K s 3) を受信すると、それを暗号エンジン 3 0 3 に送る (S 2 2 8)。暗号エンジン 3 0 3 が暗号化共通

鍵E (K P b、K s 3) を受信すると (S 2 3 0)、第1復号部3 2 1は、暗号化共通鍵E (K P b、K s 3) を自身の秘密鍵K p bで復号してチャレンジ鍵K s 3を取り出す (S 2 3 2)。つづいて、暗号エンジン3 0 3は、乱数発生部3 2 3によりセッション鍵K s 4を発生し (S 2 3 4)、暗号部3 2 2によりチャレンジ鍵K s 3でセッション鍵K s 4を暗号化して暗号化共通鍵E (K s 3、K s 4) を生成し、コントローラ3 0 1へ送る (S 2 3 6)。コントローラ3 0 1は、暗号化共通鍵E (K s 3、K s 4) を受信すると (S 2 3 8)、ストレージデバイス2 0 0に対してセッション鍵入力命令を発行する (S 2 3 9)。

【0070】

コントローラ2 0 1は、セッション鍵入力命令を正常に受理すると、暗号化鍵E (K s 3、K s 4) の入力要求をコントローラ3 0 1に出力する (S 2 4 0)。コントローラ3 0 1は、この入力要求に応じて、コントローラ2 0 1に暗号化鍵E (K s 3、K s 4) を出力する (S 2 4 2)。コントローラ2 0 1は、暗号化鍵を受信すると (S 2 4 4)、それをデータレジスタ2 2 0に格納し (S 2 4 6)、受理通知をコントローラ3 0 1に返す (S 2 4 8)。制御部2 2 2は、状態レジスタ2 2 1の処理状態を「B u s y」に変更し (S 4 2 0)、データレジスタ2 2 0からチャレンジ鍵K s 3を読み出し、第2復号部2 2 9に受信した暗号化共通鍵E (K s 3、K s 4) とチャレンジ鍵K s 3を与える。第2復号部2 2 9は、チャレンジ鍵K s 3で暗号化共通鍵E (K s 3、K s 4) を復号してセッション鍵K s 4を取り出し (S 4 2 2)、データレジスタ2 2 0にセッション鍵K s 4を格納する (S 4 2 4)。制御部2 2 2は、処理が終了すると、状態レジスタ2 2 1の処理状態を「R e a d y」に、処理結果を「N o r m a l」に変更する (S 4 2 6)。

【0071】

コントローラ3 0 1は、セッション鍵入力命令の受理通知を受け取ると、ストレージデバイス2 0 0がセッション鍵入力命令の実行に要すると推定される時間待機する (S 2 5 0)。セッション鍵入力命令の実行に要すると推定される時間が経過すると、コントローラ3 0 1は、ストレージデバイス2 0 0に対してライセンス読出命令を発行する (S 2 5 2)。このとき、読み出すべきライセンスデ

ータのアドレスが指定される。コントローラ 201 は、ライセンス読出命令を正常に受理すると、ライセンス読出命令の受理通知をコントローラ 301 に返す (S254)。制御部 222 は、状態レジスタ 221 の処理状態を「B u s y」に変更し (S430)、機密データ記憶部 205 の指定されたアドレスからライセンスデータを読み出し、データレジスタ 220 に保持する (S432)。制御部 222 は、処理が終了すると、状態レジスタ 221 の処理状態を「R e a d y」に、処理結果を「N o r m a l」に変更する (S434)。

【0072】

コントローラ 301 は、ライセンス読出命令の受理通知を受け取ると、ストレージデバイス 200 がライセンス読出命令の実行に要すると推定される時間待機する (S256)。ライセンス読出命令の実行に要すると推定される時間が経過すると、コントローラ 301 は、ストレージデバイス 200 に対してライセンス準備命令を発行する (S258)。コントローラ 201 は、ライセンス準備命令を正常に受理すると、ライセンス準備命令の受理通知をコントローラ 301 に返す (S260)。制御部 222 は、状態レジスタ 221 の処理状態を「B u s y」に変更し (S440)、第 2 暗号部 230 は、ライセンスデータをセッション鍵 K s 4 で暗号化してデータレジスタ 220 に保持する (S442)。制御部 222 は、処理が終了すると、状態レジスタ 221 の処理状態を「R e a d y」に、処理結果を「N o r m a l」に変更する (S444)。

【0073】

コントローラ 301 は、ライセンス準備命令の受理通知を受け取ると、ストレージデバイス 200 がライセンス準備命令の実行に要すると推定される時間待機する (S262)。ライセンス準備命令の実行に要すると推定される時間が経過すると、コントローラ 301 は、ストレージデバイス 200 に対してライセンス出力命令を発行する (S264)。コントローラ 201 は、ライセンス出力命令を正常に受理すると、暗号化ライセンスデータをデータレジスタ 220 から読み出してコントローラ 301 に出力する (S266)。コントローラ 301 は、暗号化ライセンスデータを取得すると、それを暗号エンジン 303 に送る (S268)。暗号エンジン 303 が暗号化ライセンスデータを受信すると (S270)

、第2復号部324は、セッション鍵Ks4で暗号化ライセンスデータを復号する(S272)。得られたライセンスデータは、復号器304に送られ、復号器304がコンテンツを復号するのに用いられる。以上の手順により、コンテンツを復号するためのライセンスデータが再生装置300により読み出される。

【0074】

上述した一連の暗号エンジン203のセキュアコマンドに対する処理において。処理結果として「Normal」を返す場合のみを説明したが、セキュアコマンドに対する処理において何らかの問題が発生し、処理が正常に終了しなかった場合には、制御部222は、状態レジスタ221の処理状態を「Ready」、処理結果を「Error」に変更する。さらに、暗号入出力処理の途中で、何らかのエラーが発生して処理が中断されたときに、その暗号入出力処理における手順を復元するための手段としてトランザクションログを記録している。トランザクションログを参照して、処理がどの手順まで進行していたかを確認し、エラーが発生した手順から再度実行してもよい。このときのトランザクションログの入出力も、セキュア機能を利用して行われる。そのため、トランザクションログの入出力に伴って発行される命令も、「セキュアコマンド」に該当する。ログメモリ125または231から必要なトランザクションログを検索する処理には比較的時間を要するため、記録装置100がストレージデバイス200にトランザクションログの出力命令を発行したとき、ストレージデバイス200がログメモリ231からトランザクションログを検索するのに要する時間を考慮して、待ち時間を設定するのが好ましい。

【0075】

図16は、記録装置100がストレージデバイス200にセキュアコマンドを発行し、ストレージデバイス200が受理する様子を示す。図9から図11におけるS102、S120、S132、S142、S158、S170、および図12から図15におけるS206、S218、S224、S239、S252、S258、S264がセキュアコマンドの発行と受理を行う処理である。記録装置100のコントローラ101は、ストレージデバイス200にセキュアコマンドを発行した後、ストレージデバイス200がそのセキュアコマンドを実行する

のに要すると推定される時間待機してから、次のセキュアコマンドを発行する（S500）。ストレージデバイス200のコントローラ201は、記録装置100からセキュアコマンドを受信すると（S502）、受信したセキュアコマンドが正規の発行手順で発行されているか否か確認する（S504）。正規の発行手順に従わない場合には（S504のN）、命令を受理することができないため処理を終了するためにS516へ進む。正規の発行手順に従っている場合には（S504のY）、状態レジスタ221を参照して、その処理系の直前の命令がまだ実行中か否かを確認する（S506）。状態レジスタ221の処理状態が「Busy」であれば、直前の命令を実行中であるから、記録装置100へ処理中である旨を通知する（S508）。コントローラ101は、ストレージデバイス200から処理中である旨の通知を受信すると（S510）、さらに所定の時間待機した後（S512）、再度S500に戻り、セキュアコマンドを発行する。

【0076】

S504において、状態レジスタ221の処理状態が「Ready」であれば、直前の命令の実行が終了したので、直前の命令の処理結果を確認するために状態レジスタの処理結果を参照する（S514）。状態レジスタの処理結果が「Normal」であれば（S514の「Normal」）、直前の命令の実行が正常に終了したので受信したセキュアコマンドを受理して次の処理へ移る。一方、状態レジスタ221の処理結果が「Error」であれば（S514の「Error」）、直前の命令の実行が正常に終了していないので、次の処理へ移ることができないため処理を終了するためにS516へ進む。命令が正規の発行手順を守っていない場合、あるいは、直前の命令が正常に終了しなかった場合、コントローラ201は、記録装置100へエラーの通知をする（S516）。コントローラ101は、ストレージデバイス200からエラーの通知を受信すると（S518）、処理を異常終了する。

【0077】

（第2の実施の形態）

図17は、第2の実施の形態に係るデータ管理システム10の全体構成を示す。本実施の形態では、第1の実施の形態における記録装置100および再生装置

300が一つの記録再生装置400として実現されている。

【0078】

図18は、本実施の形態に係る記録再生装置400の内部構成を示す。本実施の形態の記録再生装置400は、図2に示した第1の実施の形態の記録装置100の構成と、図3に示した第1の実施の形態の再生装置300の構成の双方を備えており、同様の構成には同じ符号を付している。第1暗号エンジン103は、第1の実施の形態における記録装置100の暗号エンジン103に対応し、第2暗号エンジン303は、第1の実施の形態における再生装置300の暗号エンジン303に対応する。第1暗号エンジン103の内部構成は、図5に示した第1の実施の形態の暗号エンジン103と同様であり、第2暗号エンジン303の内部構成は、図6に示した第1の実施の形態の暗号エンジン303の内部構成と同様である。コントローラ401は、第1の実施の形態における記録装置100のコントローラ101と再生装置300のコントローラ301の双方の機能を有する。ストレージインタフェース402は、ストレージデバイス200とのデータの入出力を制御し、データバス410は、記録再生装置400の構成を電氣的に接続する。

【0079】

本実施の形態の記録再生装置400の動作も、第1の実施の形態と同様であり、第1の実施の形態で説明した動作において、記録装置100を記録再生装置400に、暗号エンジン103を第1暗号エンジン103に、コントローラ101をコントローラ401に、再生装置300を記録再生装置400に、暗号エンジン303を第2暗号エンジン303に、コントローラ301をコントローラ401にそれぞれ置き換えたものと同様である。

【0080】

(第3の実施の形態)

図19は、第3の実施の形態に係る記録装置100の内部構成を示す。本実施の形態では、第1の実施の形態における記録装置100が、コンテンツを配信する配信サーバ150とコンテンツの提供を受ける端末装置160として実現されている。配信サーバ150は、暗号エンジン103、通信装置152、コンテン

ッデータベース153、ライセンスデータベース154、ユーザデータベース155、それらを制御するコントローラ151、およびそれらを電氣的に接続するデータバス156を備える。端末装置160は、コントローラ101、ストレージインタフェース102、通信装置162、およびそれらを電氣的に接続するデータバス166を備える。配信サーバ150と端末装置160は、それぞれ通信装置152および162を介して、ネットワークの一例としてのインターネット20により接続される。配信サーバ150の暗号エンジン103は、第1の実施の形態の暗号エンジン103と同様の機能を有し、端末装置160のコントローラ101およびストレージインタフェース102は、それぞれ第1の実施の形態のコントローラ101およびストレージインタフェース102と同様の機能を有する。

【0081】

コンテンツデータベース153は、ユーザに提供するコンテンツを保持する。ライセンスデータベース154は、コンテンツを暗号化するのに用いられるコンテンツ鍵を含むライセンスデータを保持する。本実施の形態では、コンテンツは既にコンテンツ鍵により暗号化されてコンテンツデータベース153に格納されているが、コンテンツデータベース153に暗号化される前のコンテンツデータを格納しておき、配信サーバ150に第1の実施の形態におけるコンテンツエンコード105および暗号器104をさらに設け、コンテンツデータベース153からコンテンツを読み出してエンコードし、暗号化してもよい。ユーザデータベース155は、コンテンツを提供するユーザの情報を保持する。たとえば、ユーザの個人情報、端末装置160のアドレス、コンテンツの購入履歴、課金情報などを保持してもよい。コントローラ151は、ユーザからの要求に応じて暗号化されたコンテンツをコンテンツデータベース153から読み出してユーザに提供する。そして、暗号エンジン103によりそのコンテンツを復号するためのライセンスデータがユーザに提供されると、そのコンテンツの対価を課金すべくユーザデータベース155を更新する。

【0082】

本実施の形態の暗号入出力処理の手順は、第1の実施の形態と同様である。本

実施の形態では、暗号エンジン 103 とコントローラ 101 との間の通信がインターネット 20 を介して行われるので、同一装置内で通信が行われる第 1 の実施の形態に比べてよりデータの漏洩の危険性が増すが、図 9 から図 15 で説明したように、暗号エンジン 103 とコントローラ 101 との間でも必ずデータを暗号化して送受信を行うので、高い耐タンパ性を実現することができる。

【0083】

(第 4 の実施の形態)

図 20 は、第 4 の実施の形態に係る端末装置 160 の内部構成を示す。本実施の形態は、第 3 の実施の形態における端末装置 160 が、一方のストレージデバイス 200 からライセンスデータを読み出し、他方のストレージデバイス 200 へ転送する例を示す。すなわち、端末装置 160 は、一方のストレージデバイス 200 には再生装置 300 として、他方のストレージデバイス 200 には記録装置 100 として機能する。それぞれの場合の動作については、第 1 の実施の形態と同様である。

【0084】

以上、本発明を実施の形態をもとに説明した。この実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【0085】

実施の形態では、暗号エンジン内において暗号化や復号を行う機能ブロックを別に示したが、それらの構成要素において回路を共有してもよい。これにより、ハードウェア規模を抑え、小型化、低消費電力化に寄与することができる。

【0086】

【発明の効果】

本発明によれば、記録装置とホスト装置との間で秘匿すべきデータを暗号化して入出力するときの処理効率を向上させることができる。

【図面の簡単な説明】

【図 1】 第 1 の実施の形態に係るデータ管理システムの全体構成を示す図

である。

【図 2】 第 1 の実施の形態に係る記録装置の内部構成を示す図である。

【図 3】 第 1 の実施の形態に係る再生装置の内部構成を示す図である。

【図 4】 第 1 の実施の形態に係るストレージデバイスの内部構成を示す図である。

【図 5】 図 2 に示した記録装置の暗号エンジンの内部構成を示す図である。

【図 6】 図 3 に示した再生装置の暗号エンジンの内部構成を示す図である。

【図 7】 図 4 に示したストレージデバイスの暗号エンジンの内部構成を示す図である。

【図 8】 ホスト装置が、ストレージデバイスにおける命令の実行に必要な時間を推定するための情報をストレージデバイスから取得する手順を示す図である。

【図 9】 記録装置がストレージデバイスにライセンスデータを記録するまでの手順を示す図である。

【図 1 0】 記録装置がストレージデバイスにライセンスデータを記録するまでの手順を示す図である。

【図 1 1】 記録装置がストレージデバイスにライセンスデータを記録するまでの手順を示す図である。

【図 1 2】 記録装置がストレージデバイスにライセンスデータを記録するまでの A T A インタフェース上の手順を示す図である。

【図 1 3】 再生装置がストレージデバイスからライセンスデータを読み出すまでの手順を示す図である。

【図 1 4】 再生装置がストレージデバイスからライセンスデータを読み出すまでの手順を示す図である。

【図 1 5】 再生装置がストレージデバイスからライセンスデータを読み出すまでの手順を示す図である。

【図 1 6】 記録装置がストレージデバイスにセキュアコマンドを発行する

様子を示す図である。

【図 17】 第 2 の実施の形態に係るデータ管理システムの全体構成を示す図である。

【図 18】 第 2 の実施の形態に係る記録再生装置の内部構成を示す図である。

【図 19】 第 3 の実施の形態に係る記録装置の内部構成を示す図である。

【図 20】 第 4 の実施の形態に係る端末装置の内部構成を示す図である。

【符号の説明】

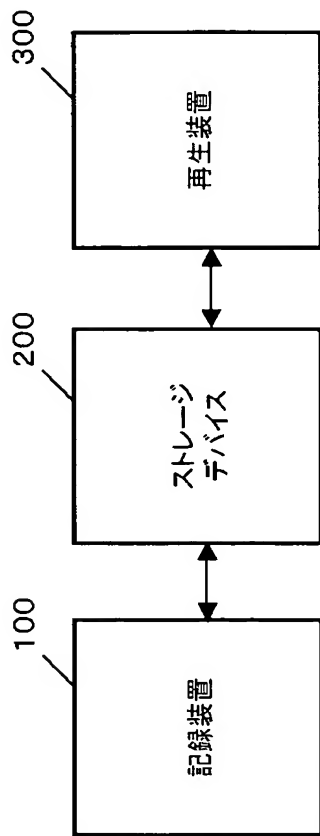
10・・・データ管理システム、100・・・記録装置、101・・・コントローラ、102・・・ストレージインタフェース、103・・・暗号エンジン、104・・・暗号器、105・・・コンテンツエンコーダ、110・・・データバス、120・・・認証部、121・・・第1暗号部、122・・・乱数発生部、123・・・復号部、124・・・第2暗号部、125・・・ログメモリ、130・・・ローカルバス、150・・・配信サーバ、151・・・コントローラ、152・・・通信装置、153・・・コンテンツデータベース、154・・・ライセンスデータベース、155・・・ユーザデータベース、156・・・データバス、160・・・端末装置、162・・・通信装置、166・・・データバス、200・・・ストレージデバイス、201・・・コントローラ、202・・・ストレージインタフェース、203・・・暗号エンジン、204・・・通常データ記憶部、205・・・機密データ記憶部、210・・・データバス、220・・・データレジスタ、221・・・状態レジスタ、222・・・制御部、224・・・乱数発生部、225・・・証明書出力部、226・・・認証部、227・・・第1復号部、228・・・第1暗号部、229・・・第2復号部、230・・・第2暗号部、231・・・ログメモリ、240・・・ローカルバス、300・・・再生装置、301・・・コントローラ、302・・・ストレージインタフェース、303・・・暗号エンジン、304・・・復号器、305・・・コンテンツデコーダ、310・・・データバス、320・・・証明書出力部、321・・・第1復号部、322・・・暗号部、323・・・乱数発生部、324・・・第2復号部、330・・・ローカルバス、400・・・記録再生装置、401・・・

・ ・ コントローラ、 4 0 2 ・ ・ ・ ストレージインタフェース、 4 1 0 ・ ・ ・ データバス。

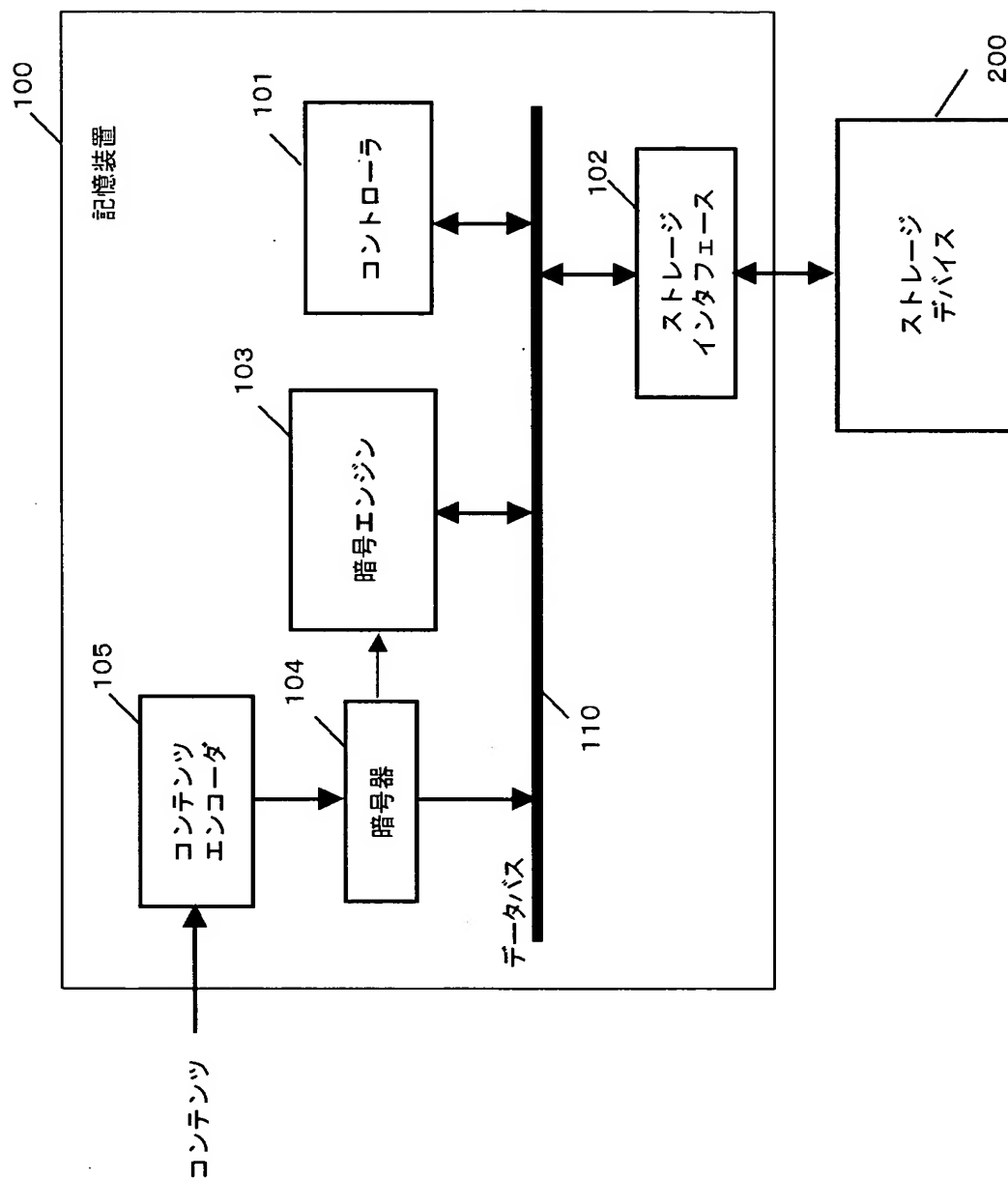
【書類名】 図面

【図 1】

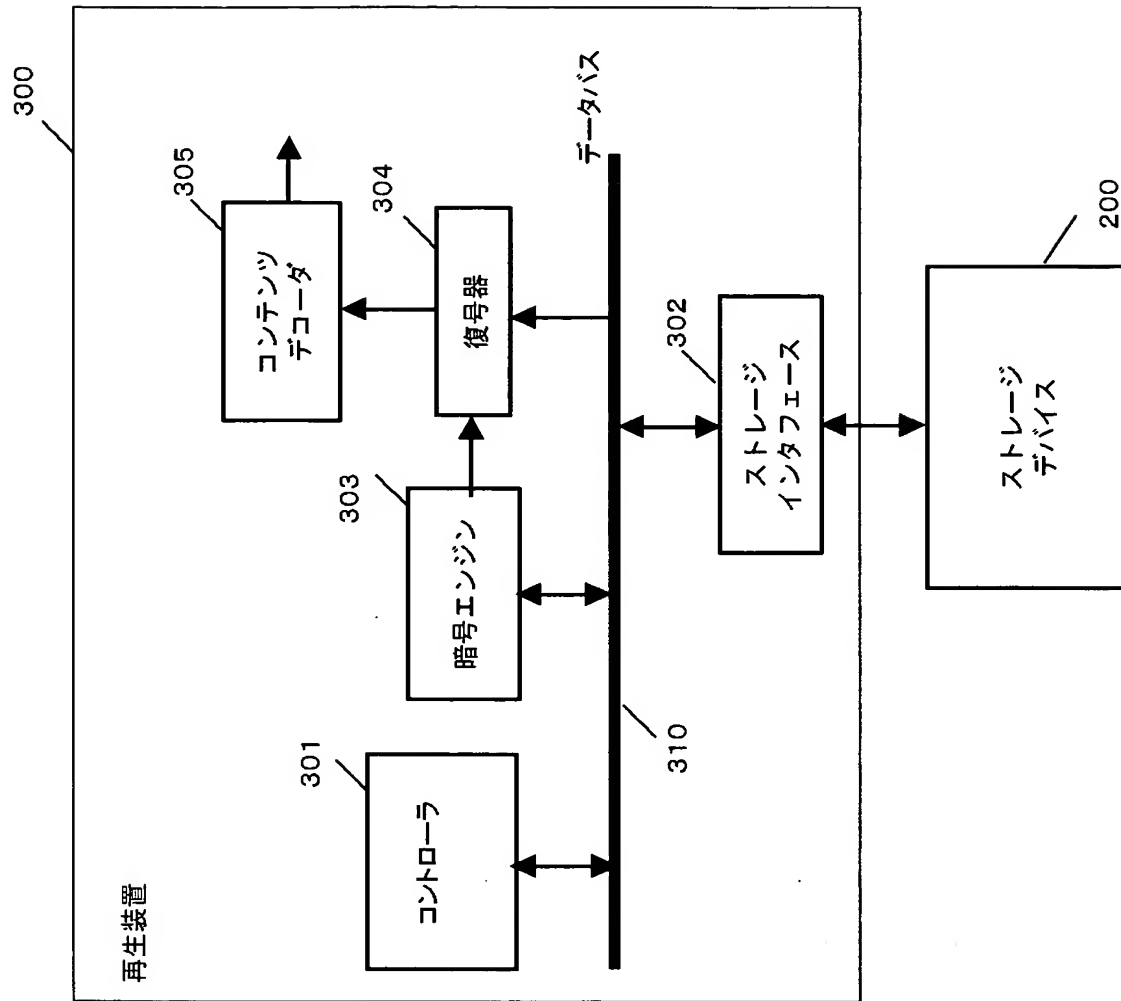
10



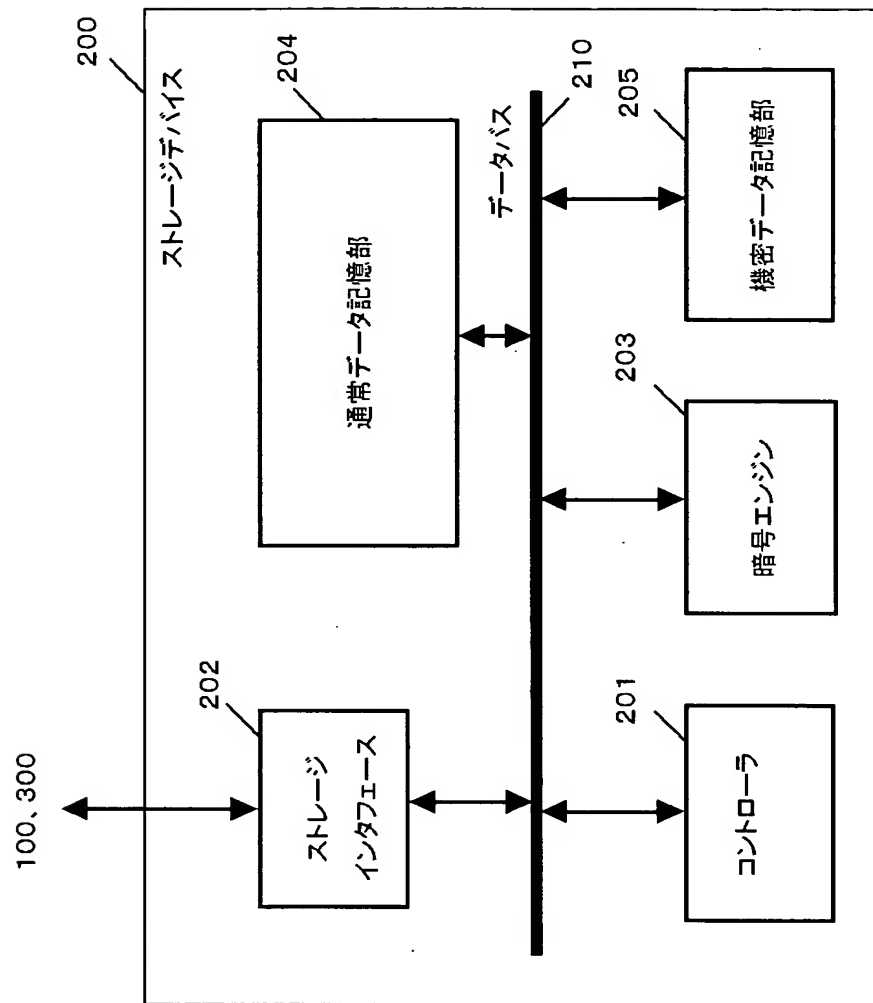
【図 2】



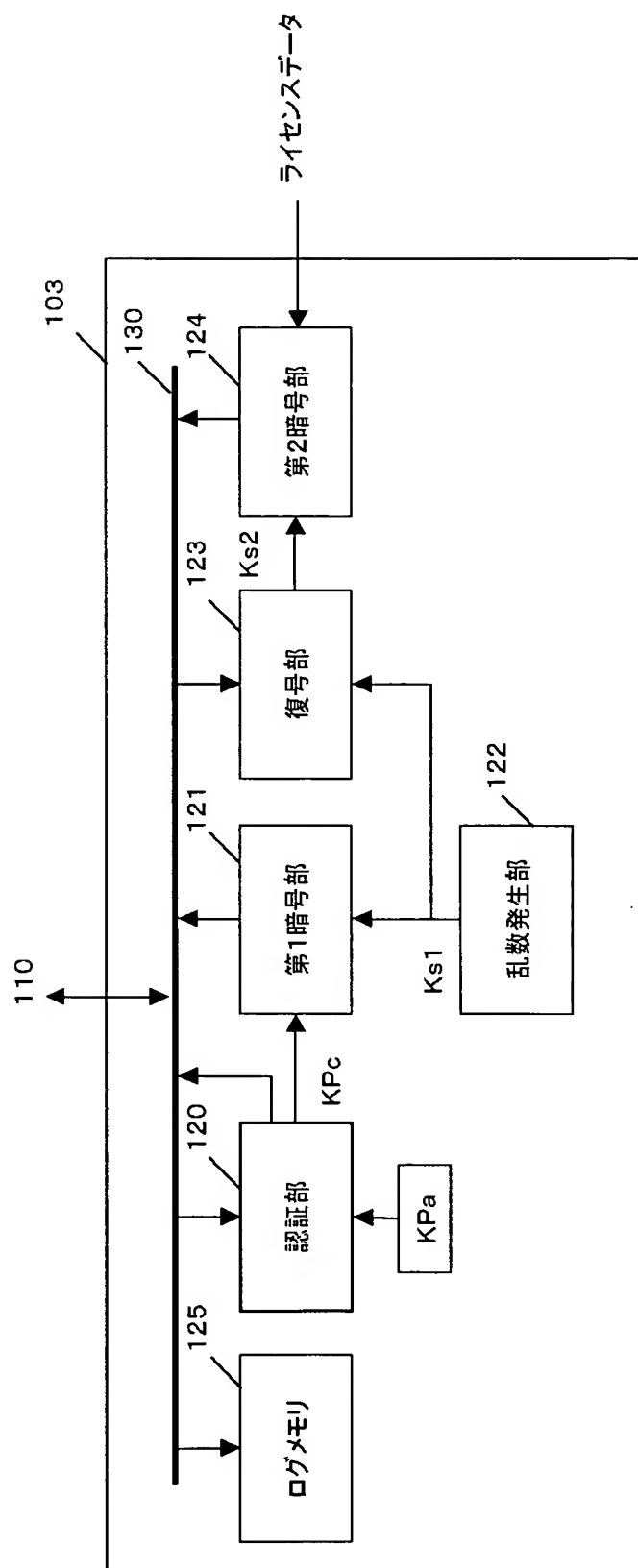
【図 3】



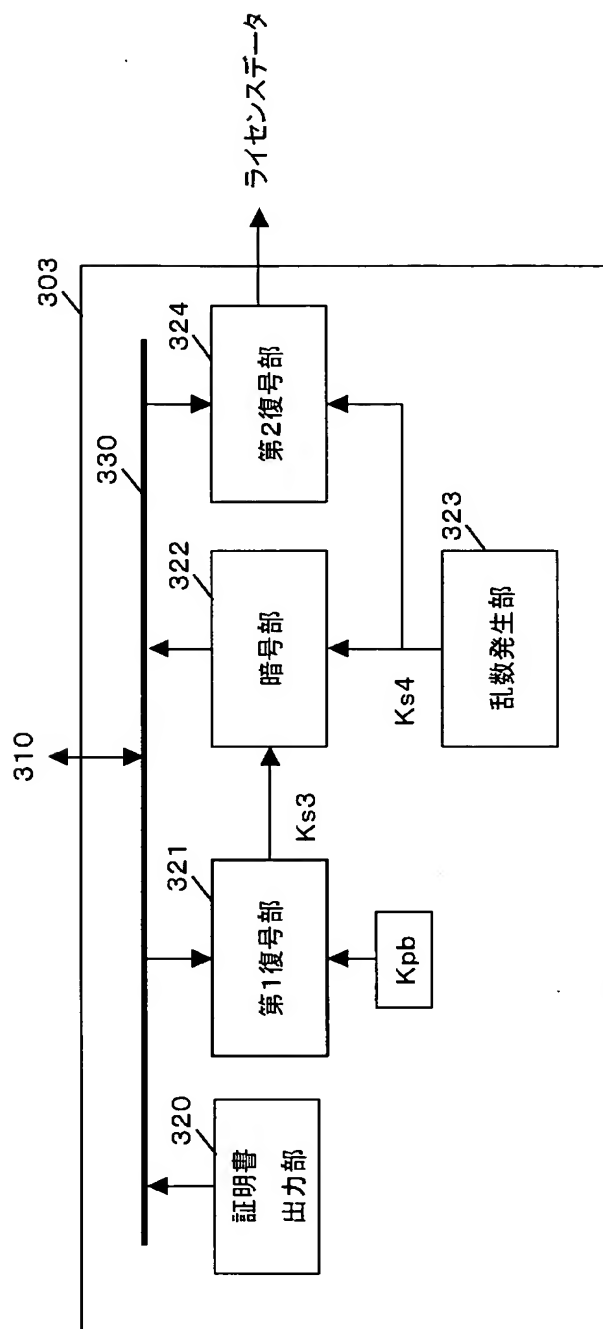
【図 4】



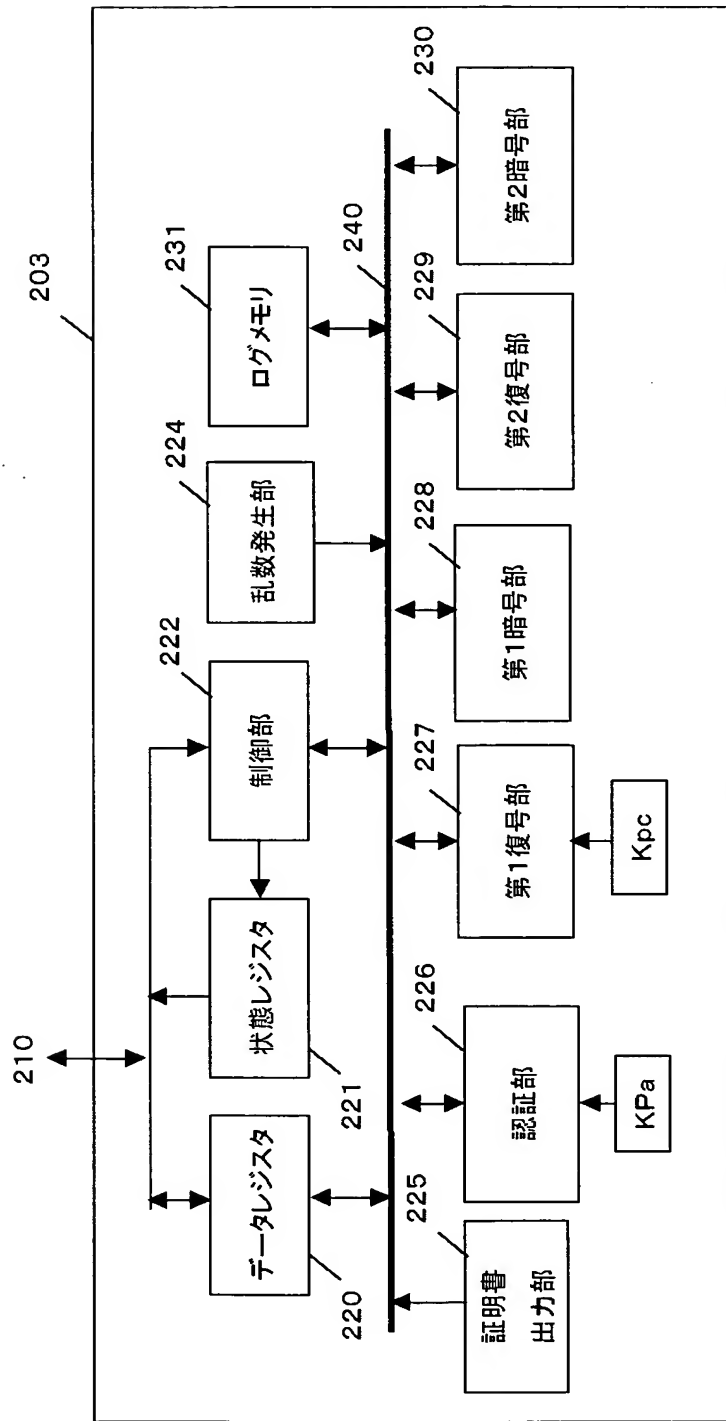
【図 5】



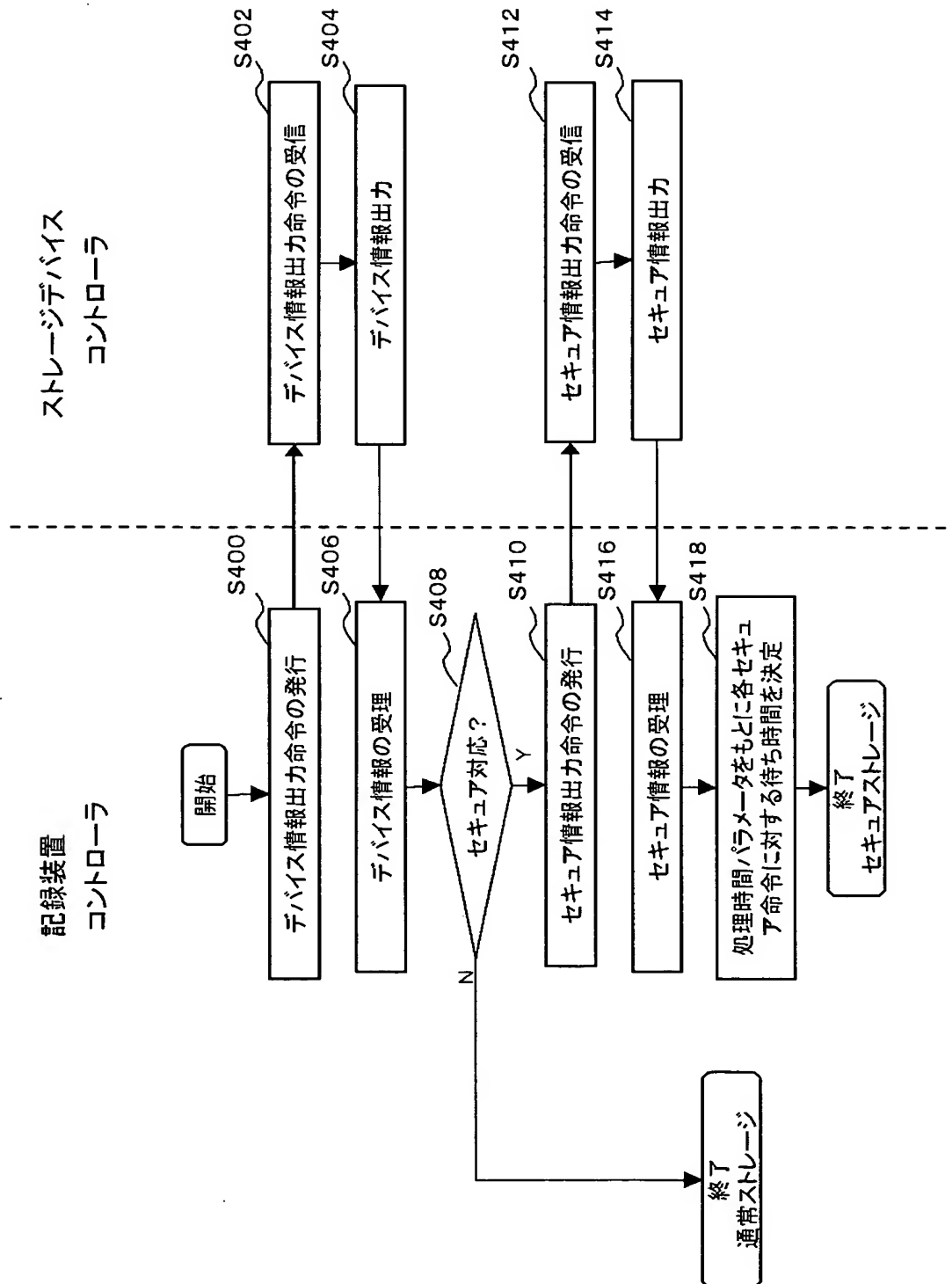
【図 6】



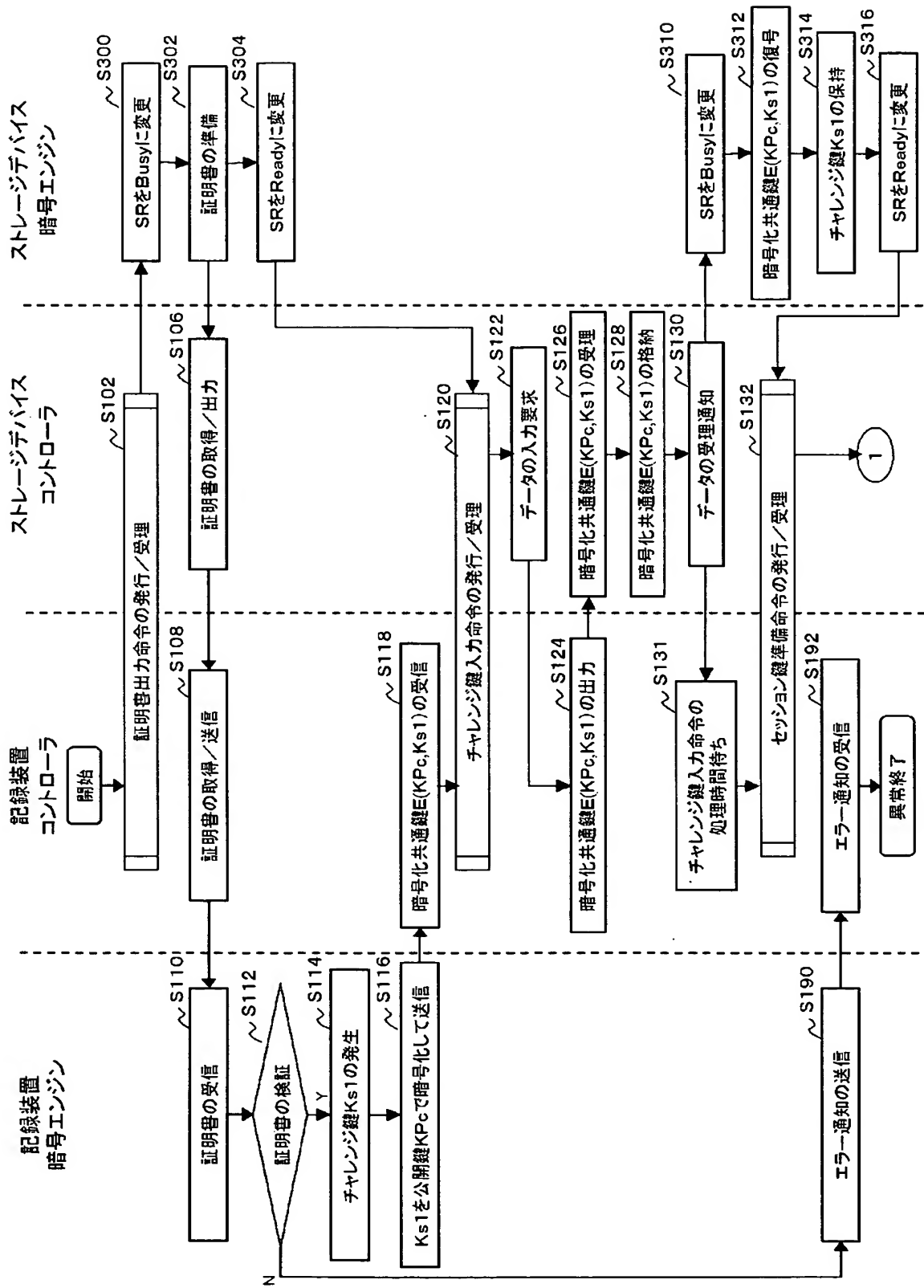
【図 7】



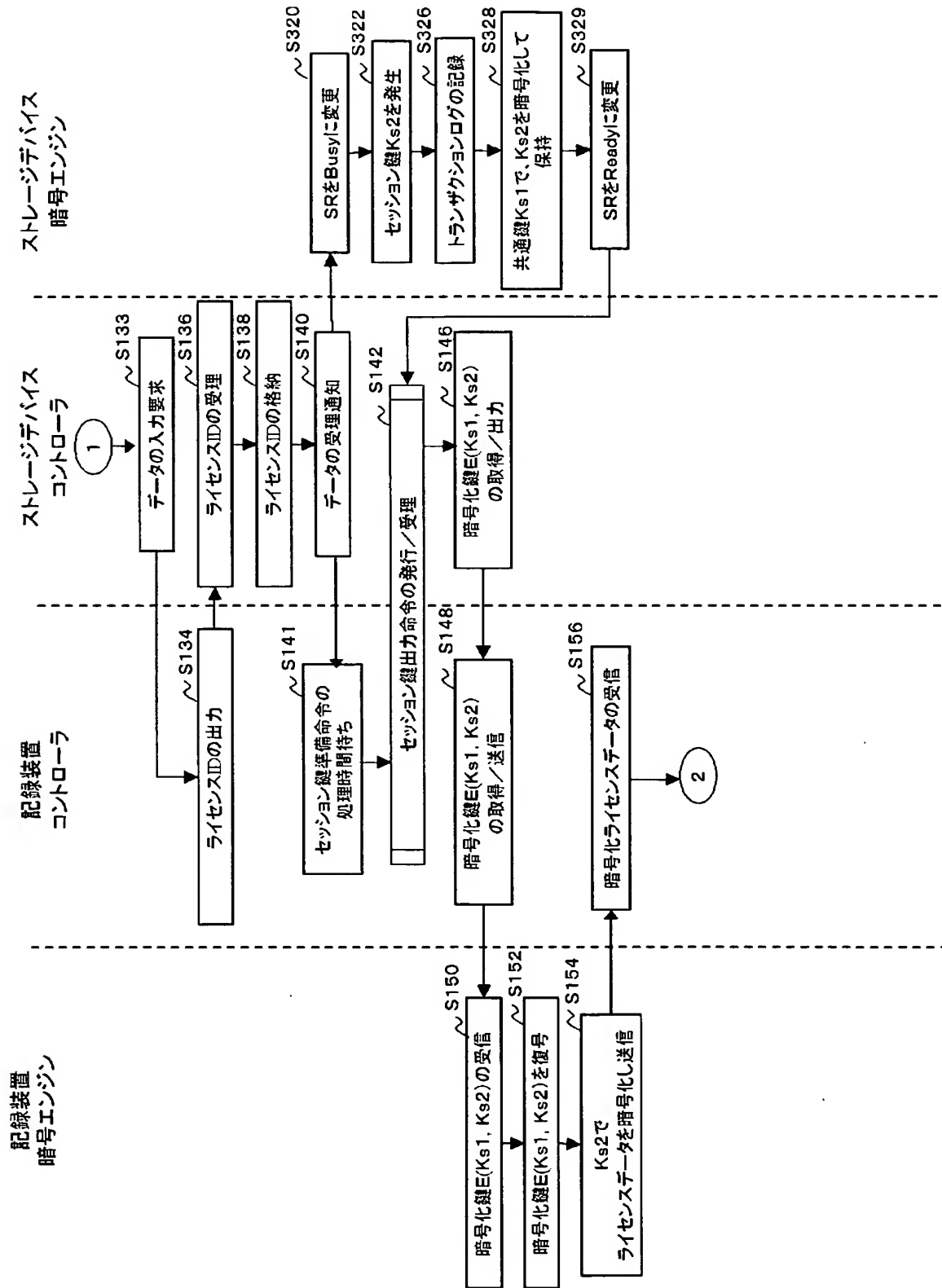
【図 8】



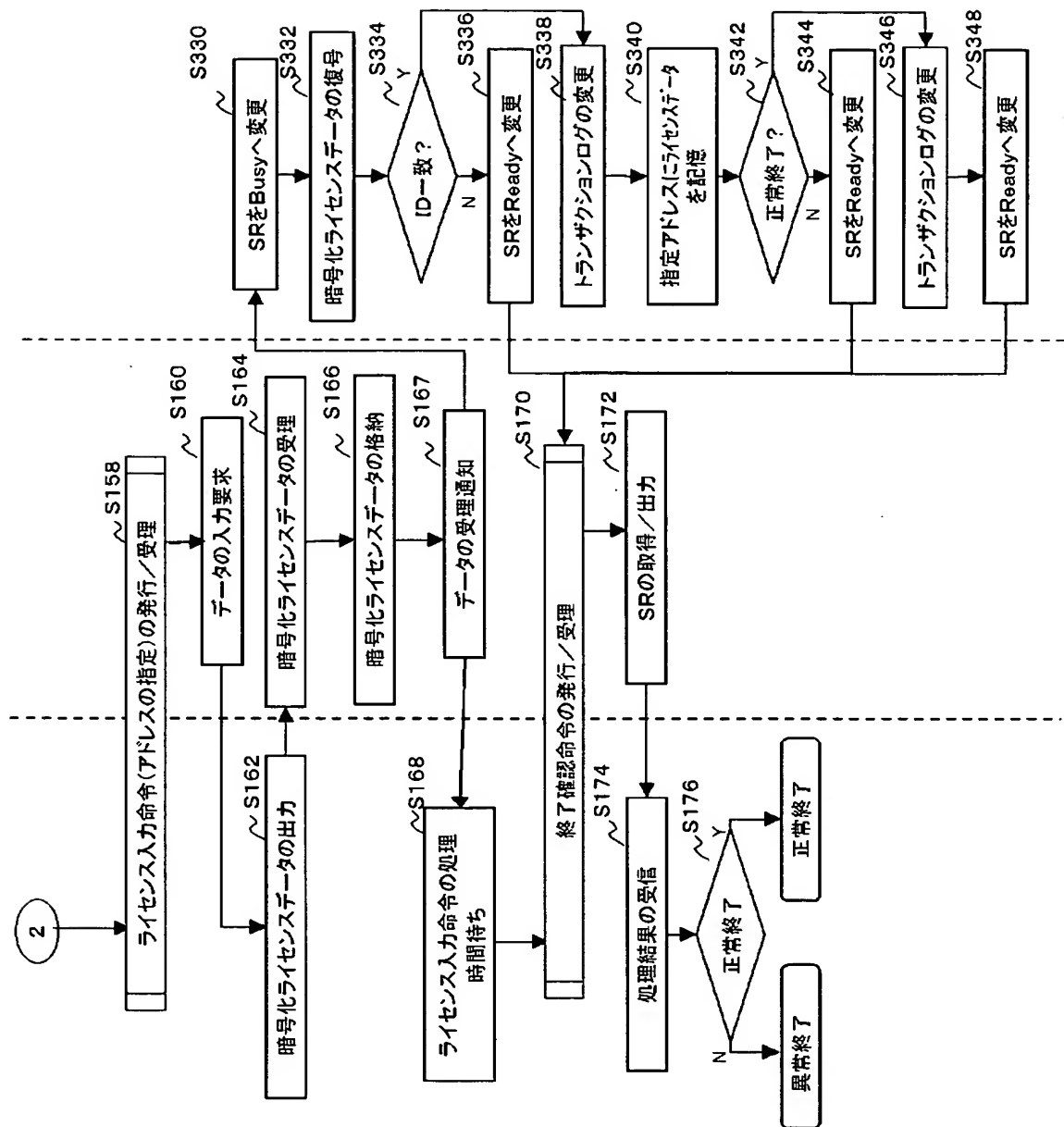
【図 9】



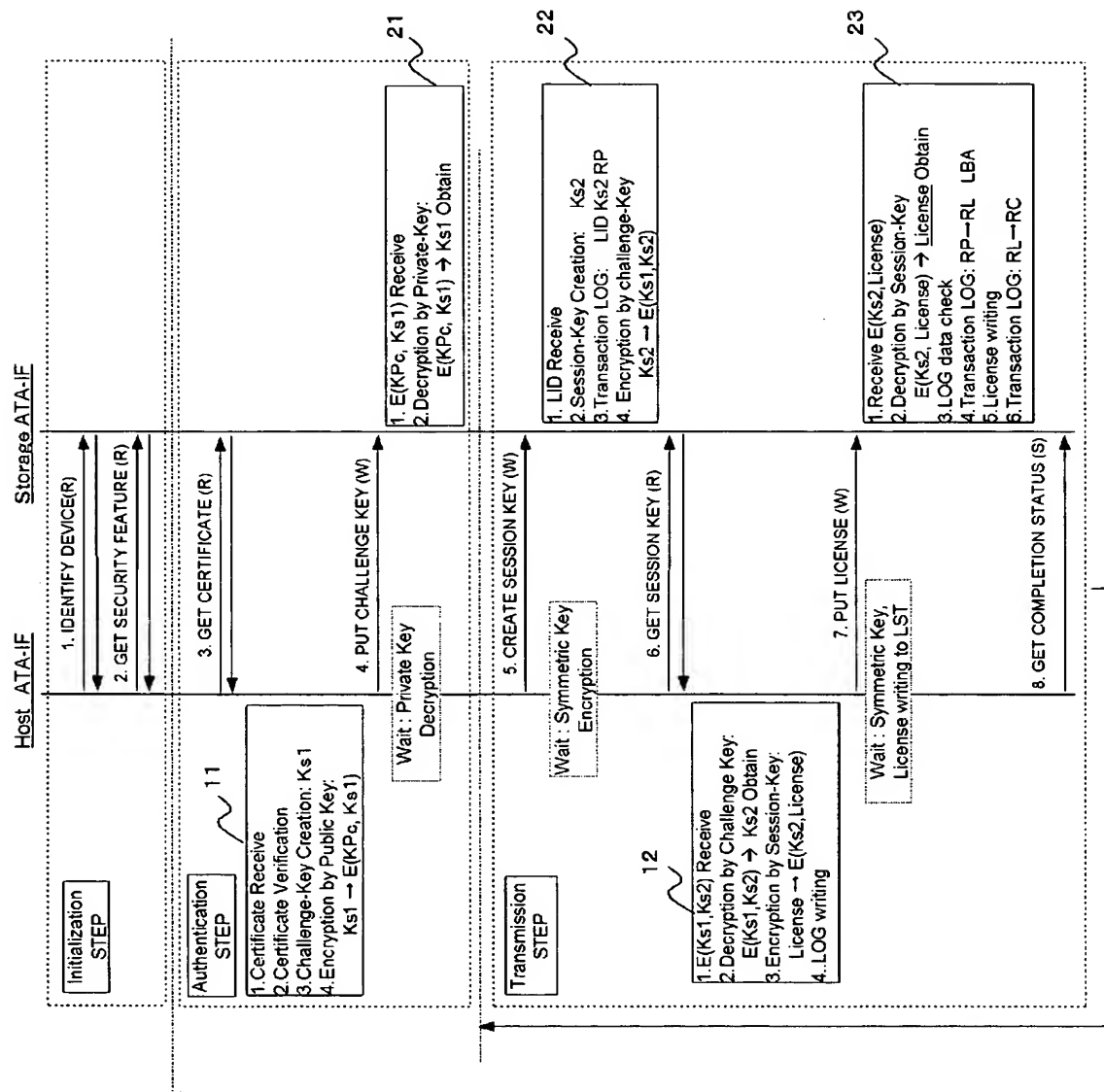
【図 10】



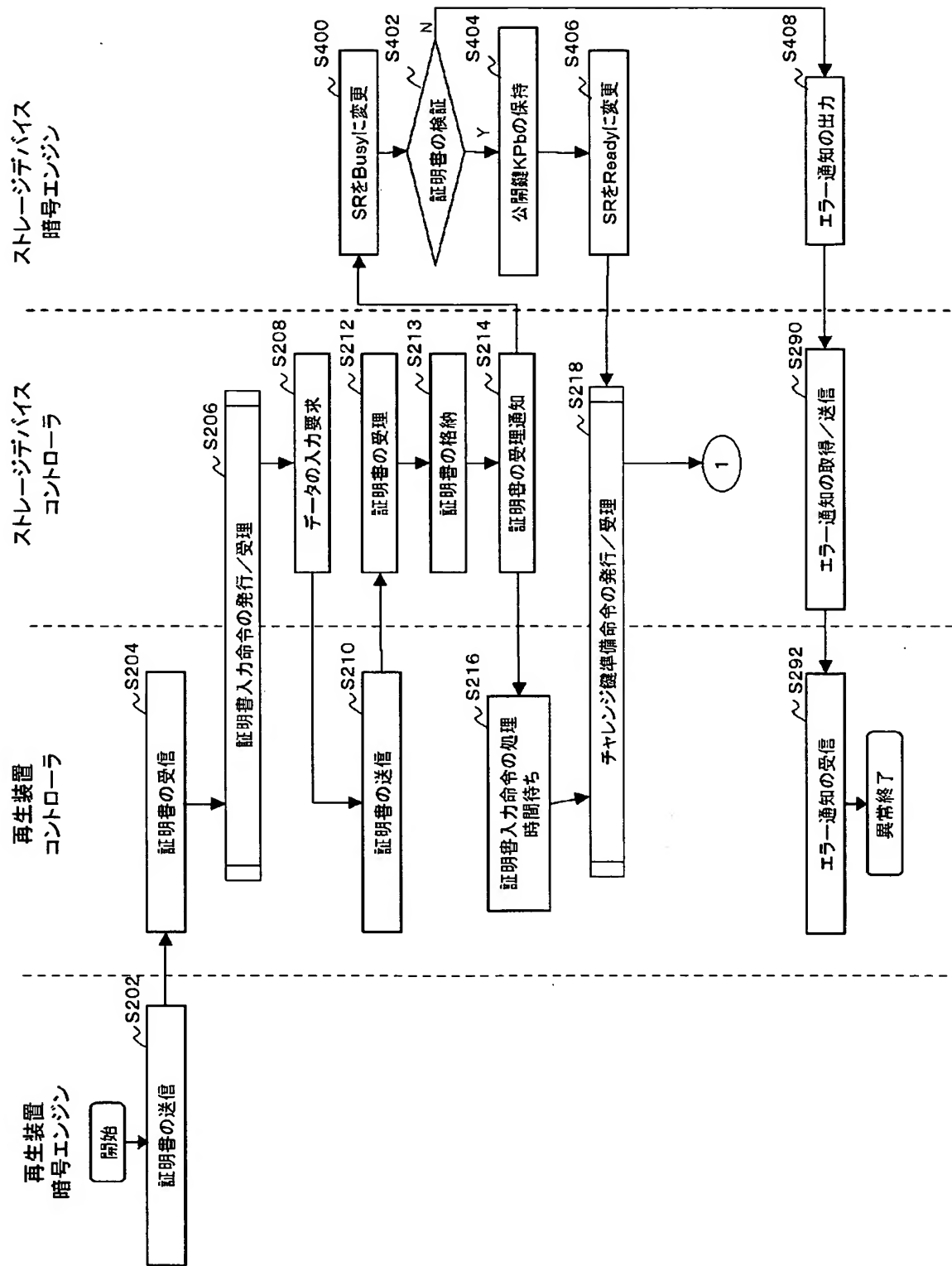
【図 11】



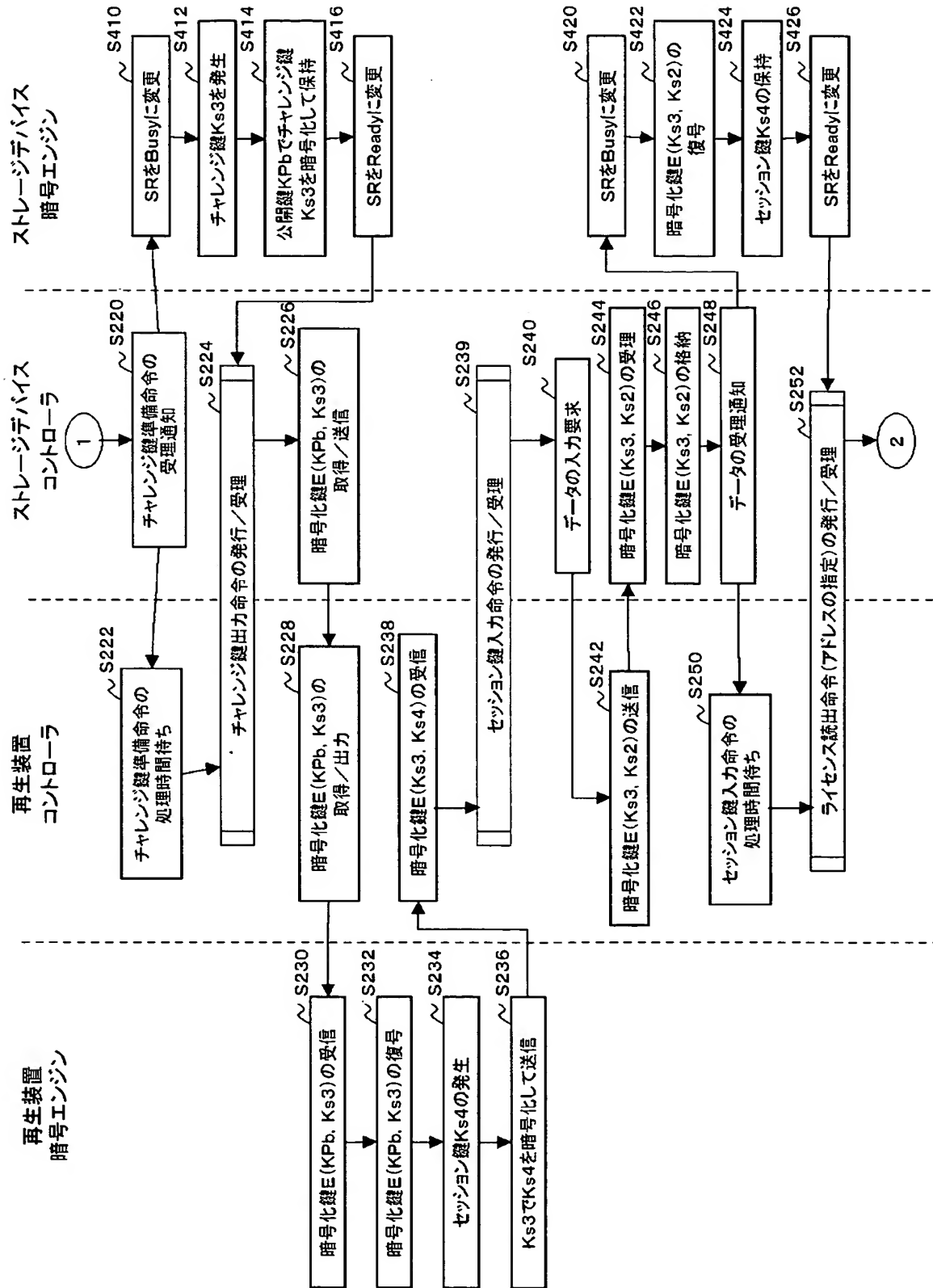
【図 12】



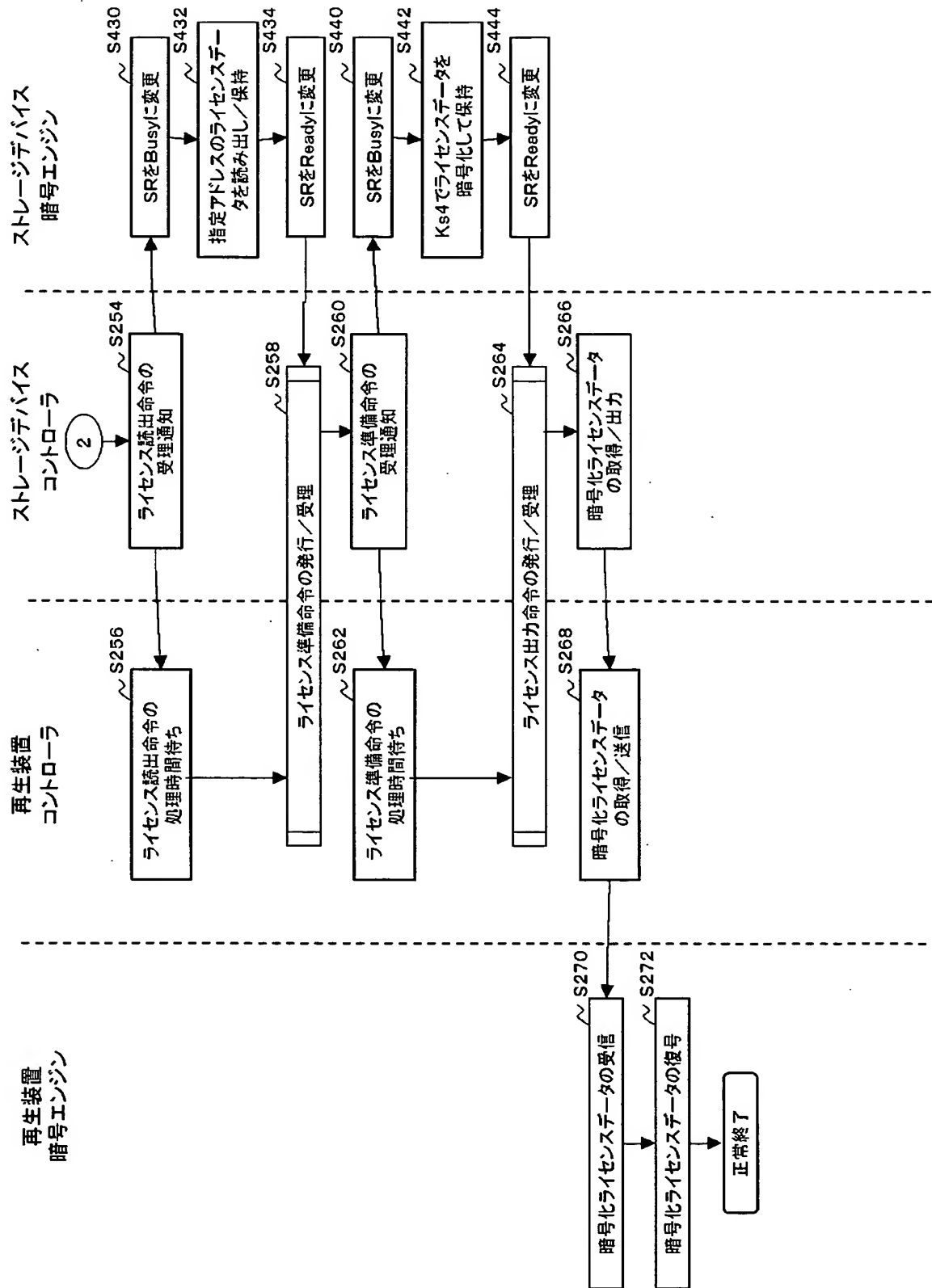
【図 13】



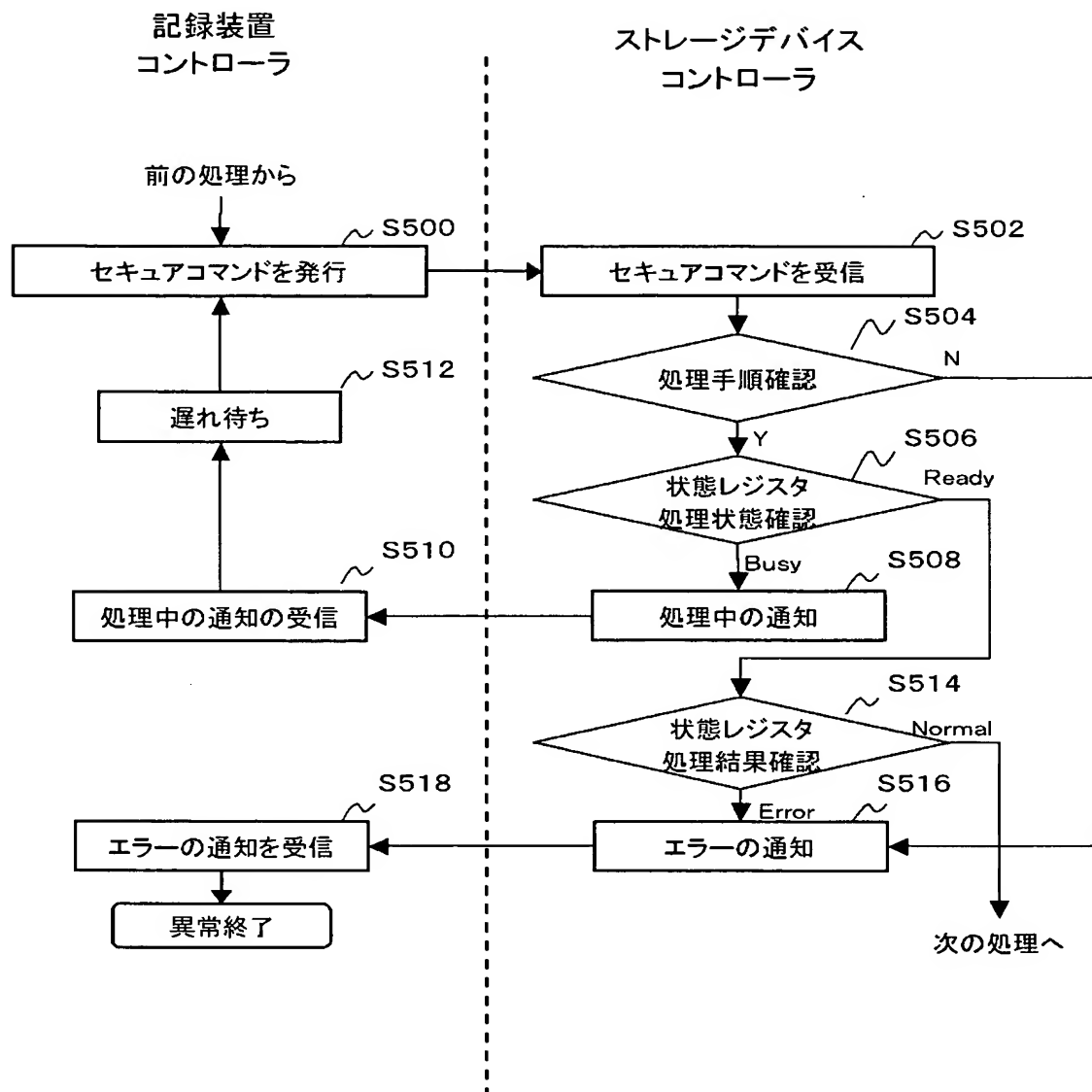
【図 14】



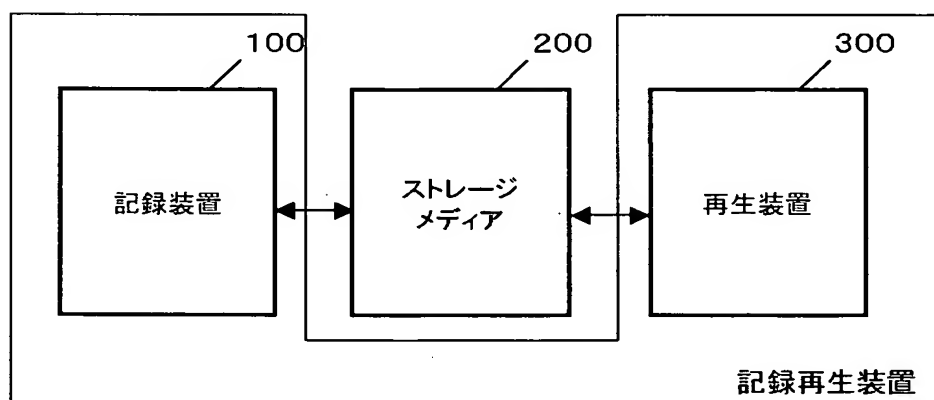
【図 15】



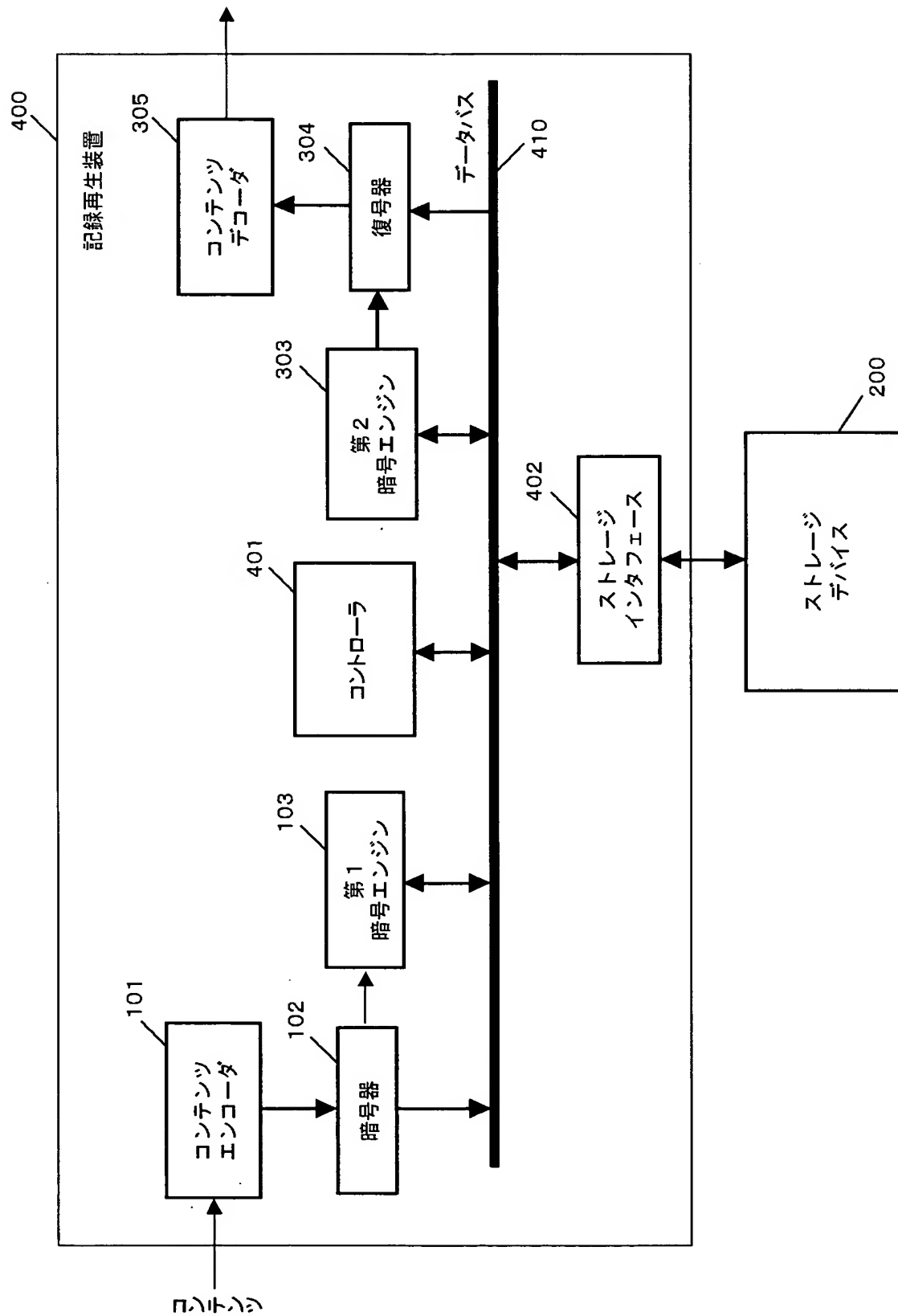
【図 16】



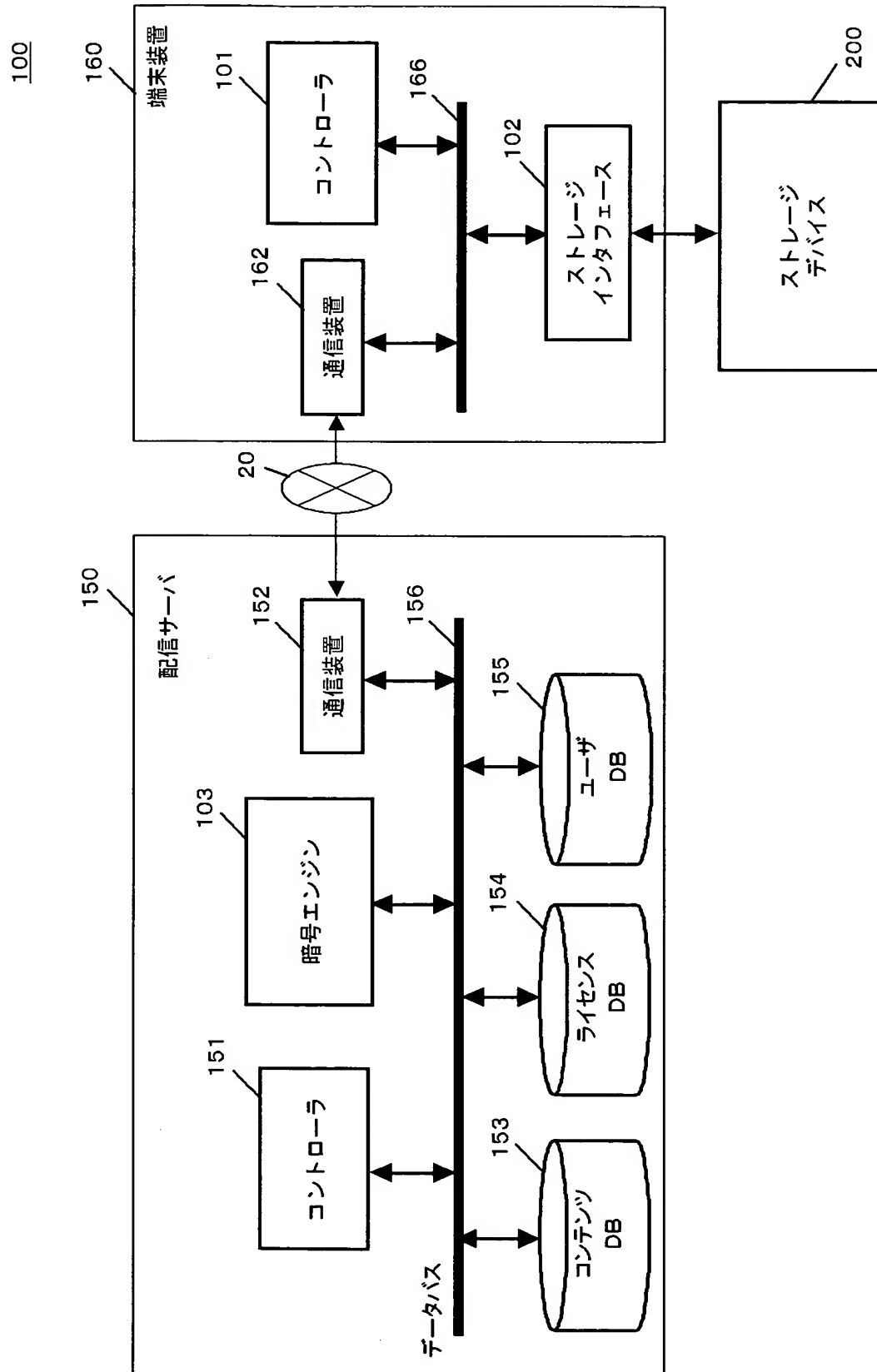
【図 17】



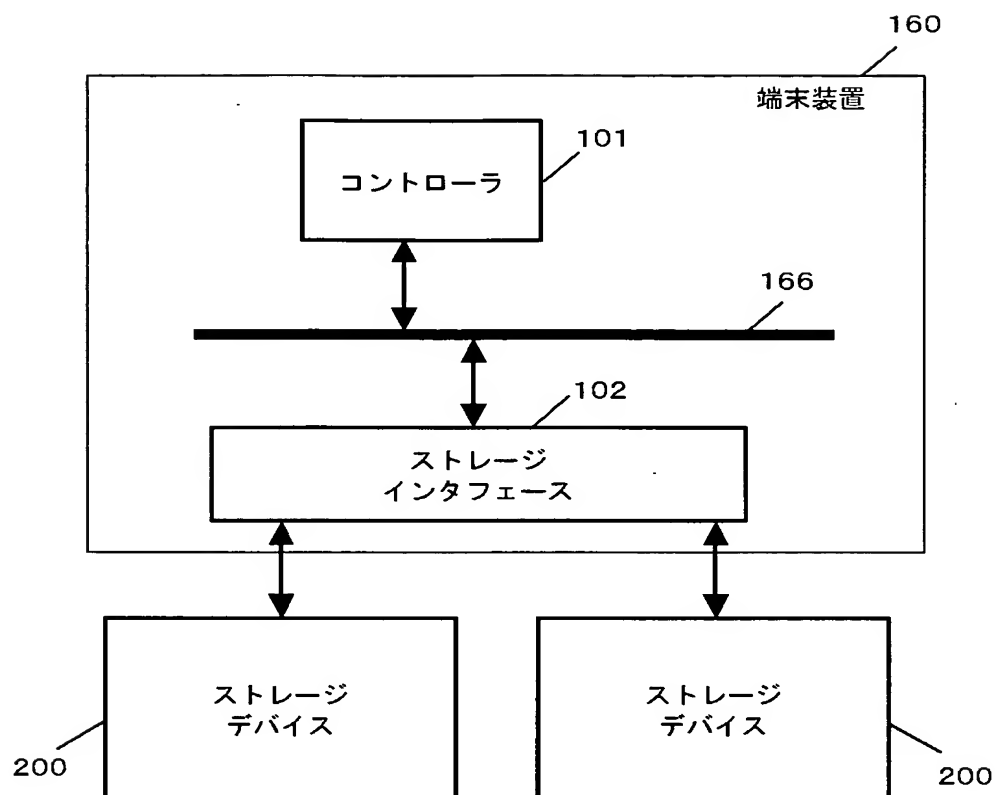
【図 18】



【図 19】



【図 20】



【書類名】 要約書

【要約】

【課題】 記録装置とホスト装置との間で秘匿すべきデータを暗号化して入出力するときの処理効率を向上させる。

【解決手段】 記録装置のコントローラは、ストレージデバイスにセキュアコマンドを発行した後、ストレージデバイスがそのセキュアコマンドを実行するのに要すると推定される時間待機してから、次のセキュアコマンドを発行する（S500）。ストレージデバイスのコントローラは、直前の命令を実行中であれば、記録装置へ処理中である旨を通知し（S508）、直前の命令の実行が正常に終了していれば、次の処理へうつる。コマンドの実行時間を推定するための情報は予めストレージデバイスから取得しておく。

【選択図】 図16

特願 2003-089388

出 願 人 履 歴 情 報

識別番号 [000001889]

1. 変更年月日 1993年10月20日

[変更理由] 住所変更

住 所 大阪府守口市京阪本通2丁目5番5号

氏 名 三洋電機株式会社

特願 2 0 0 3 - 0 8 9 3 8 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 0 4 9]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

大阪府大阪市阿倍野区长池町 2 2 番 2 2 号

氏 名

シャープ株式会社

特願 2 0 0 3 - 0 8 9 3 8 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 3 2 9]

1. 変更年月日

1 9 9 0 年 8 月 8 日

[変更理由]

新規登録

住 所

神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地

氏 名

日本ビクター株式会社

特願 2 0 0 3 - 0 8 9 3 8 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 0 1 6]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都目黒区目黒 1 丁目 4 番 1 号

氏 名

パイオニア株式会社

特願 2 0 0 3 - 0 8 9 3 8 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所

特願 2 0 0 3 - 0 8 9 3 8 8

出 願 人 履 歴 情 報

識別番号

[3 0 0 0 1 7 6 3 6]

1. 変更年月日

2 0 0 3 年 1 月 8 日

[変更理由]

住所変更

住 所

東京都千代田区丸の内 1 - 3 - 1 東京銀行協会ビル 1 4 F

氏 名

フェニックステクノロジーズ株式会社

特願 2 0 0 3 - 0 8 9 3 8 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社